Volume Twenty-Eight, Number Two
Summer 2011, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly

1 2>
7 25274 83158 6

Foreign Payphones

Albania. Seen in the capital city of Tirana, this is the standard model that takes only cards. And yes, "Shqiptar" is an ethonym for the Albanian language. But you knew that.

Photo by Kyle Drosdick

Israel. This bright orange and black model can be found in Jerusalem and does not take coins. We firmly believe that colorful payphones brighten everyone's day.

Photo by FA

Iran. Both of these very different models are used in the streets of Tehran. One is old and takes coins, one is newer and takes cards. But they each exist under the exact same style of canopy. There's probably a lesson in here somewhere.

Photos by Venture37

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

Eye Candy

Progress Report	4
Dealing with Credit Card Companies	6
Detecting and Tracking Stealth Satellites	7
Pen Testing from a Mile Away	9
Securing Online Voting	11
TELECOM INFORMER	13
Mobile Hacking with Android	15
How I Escaped Google	20
Add a User With Root Privileges Non-Interactively	22
Simple RSA Encryption	23
Booze, Nosiness, and City Terminals	25
HACKER PERSPECTIVE	26
How to Protect Your Car from Radio Jammers	28
POCSAG and Radio Privacy	29
Auditing the MiFi2200	32
LETTERS	34
Hiding the Hacker Instinct	47
Starting a Path to Modern Database Privacy	48
TRANSMISSIONS	52
A Brief Guide to Black Edition XP	54
The Many Uses of SSH Tunnels	56
Senatorial Courtesy Plates - An Inside Look	58
Fishing with Squid	59
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

It's been a mere six months since we began offering electronic subscriptions to *2600* via the Kindle, and not much longer since we created our first digital edition last autumn. We mentioned in these pages that this was an experiment for us, and perhaps for the publishing world in general. We also promised to keep our readers in the loop as we tested the waters and experimented a bit. While there is still much to be learned, what has already happened is fairly enlightening.

The response so far has been nothing short of staggering. It only took a couple of months for digital subscriptions to shoot past paper subscriptions in number, with many more coming in every day. We attribute this to several factors:

- It's extremely easy to subscribe. Literally, a couple of clicks and the content is there on your Kindle and automatically updated.
- There has been a lot of word of mouth. We've been trying to approach this in our own unique way so that our readers are involved in the process and ensuing evolution. This has gotten a good degree of attention from the public as well as other publications since the results we get could very well portray what the future landscape will be.
- We stand out in a relatively small field. What we're doing is dangerous in the eyes of those who fear innovation and change. Unfortunately, that represents a large number of existing publishers, as well as entities used to an older way of doing things. This is why, to this day, there are only a few dozen magazines represented on the Kindle.

To us, this proves beyond any doubt that readers will support a publication electronically as well as physically if the content is of interest and the price is reasonable. Neither of these conditions is a given, however. We've encountered books and publications that obscenely overprice their electronic content. We've seen downloadable CDs that are more expensive than the physical CD itself - often from the same online source. There is no better way to drive people away than to treat them with this kind of disrespect. Rather than fear the consumer and try to take advantage of them as much as possible, publishers of words, music, film, etc. need to connect with them and remember why they're doing this in the first place.

All of that said, the Kindle is but one device with certain limitations. There are a number of other devices and formats that we're trying to work with as well. But there are some inevitable growing pains.

Every format requires a different conversion process and all sorts of potential for mishaps. This will have to improve over time. What's a lot more annoying is the way we have to get embroiled in the battles that providers like Amazon, Apple, and Google are having between themselves. For instance, we have to provide the lowest price to Amazon or our payment from them gets cut in half. Other

services, such as the Barnes & Noble Nook, set the price of a subscription themselves, meaning they could undercut Amazon without our consent and then we'd be screwed. So the solution for now is not to offer a subscription in that way, much as we want to. (Issues can only be obtained individually on the Nook.) As of press time, an agreement still hasn't been reached that would allow Kindle magazine subscriptions to be readable on iPads and other Apple devices. Again, we're offering the issues individually in order to get around this. Recently, it was announced by Amazon that we no longer supported Android devices when it was actually Amazon's decision (or mistake) to do this. We were pretty outraged, as were many of our readers who had already subscribed using those devices. By the time Amazon got it sorted out, we had already amassed enough negative reviews to knock us out of the Number One spot we had held in customer satisfaction. (Apparently, you can only rate the publisher, not the provider.) In addition, to this day there's a prominent notice on our subscription page that says "We [Amazon] will share the name, billing address, and order information associated with your newspaper or magazine purchase with the publisher, who is under obligation to keep that information confidential." We can assure you that we've never had access to any of this information and have been told - in direct contradiction to the above - that it's against their policy to share this information. It would be rather handy if we had access to it, as we could then be more inclusive of our electronic readers by offering them subscriber-only features such as free marketplace ads. These kinds of bumps in the road make things harder than they really have to be and they can't be doing much to encourage more publishers to try out the new technology.

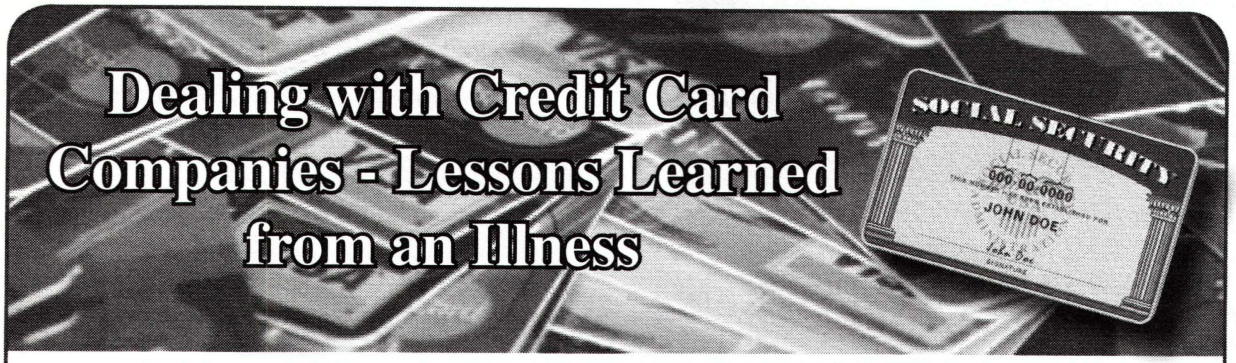
We've also been experimenting with new formats, such as our annual 300 page collection of articles and expanded pictures in PDF format. The reaction to last year's *Volume 26* was strong enough to get us to do it again for *Volume 27.* For each of these projects, it's vital that everything be done properly, which takes more time than we had ever anticipated. But in the end, that's a good thing because we wind up with something unique that we're proud of and it provides a service for those who want the magazine in this format. We also have a bit more control over pricing and publishing conditions, meaning that we can do this cheaply and with absolutely no digital rights management (DRM) controls. (We insist on this for all of our projects, but sometimes a provider does something that goes against our wishes, in which case we're forced to complain and drag their name through the mud.)

It doesn't have to end there. This is a new landscape and we can populate it with original ideas and features that would have been difficult before. As always, we're open to feedback on this. It may take time to get things working just right, but we seem to be well on the way, and in a relatively short amount of time.

All of this is not meant to take away from the importance of our trusty paper edition. We believe there will always be a strong market for our kind of material in a printed magazine and that there's something special and unique about our publication when it appears in mailboxes or on bookshelves. We don't want to ever lose that thrill. But that's how things change in a positive way - new facets of technology merge with the old ways of doing things and we end up with multiple outlets that complement each other and make the entire experience that much more fulfilling.

We've learned so much in the last half a year and it seems there is a good deal more ahead. We need to take this method of achievement and apply it everywhere else that our interests lie, not just in the places where we're expected to go. For example, rather than accept limitations of technology as defined by our own expectations of how the door will be closed in our faces, why not start the dialog and reach for something new? If, say, hacker conferences in Europe can get phenomenal amounts of bandwidth donated to them by their phone companies, why must we assume that such a thing could never happen here? If the media continues to misunderstand and misreport what the hacker world is all about, why do we conclude that we will never be able to sway the perspective in a totally different direction? Sure, any such achievement is an incredible challenge and requires a lot of people working together. But it can only be attained if the effort is expended and if there is a belief that those things everyone believes are impossible can be completely doable with some determination and cleverness. This is how hackers have always accomplished things. We know how to do it on an individual and local level. Naive as it may sound, we can reach much higher and eventually see even more accomplished.

Dealing with Credit Card Companies - Lessons Learned from an Illness



by The Piano Guy

In the event of illness and loss of ability to conduct your own affairs, someone is going to have to manage your financial situation. If you're the stereotypical reader of this great magazine, it is at least as likely that you will be doing this for someone else, most likely an aging parent. That includes dealing with credit card companies. Hacker-oriented lessons were learned, hence this article.

As usual, there is information in here that can be used for nefarious purposes. Please don't. Electricity can cook a meal for a man, or can cook the man. Use these tools wisely. Also, this article gets better towards the end, but there is information in here that I want you to read, so please eat your veggies before going to dessert.

My story starts with mom falling down a flight of stairs and breaking her neck (C2 and C7), shoulder, scapula, and three ribs. From there, it goes downhill. After the third surgery, they had to bury her in enough Haldol that dementia kicked in. On advice of the attorney, before this happened we had her sign over her rights using a General Power of Attorney (POA) and Medical Power of Attorney (MPOA). These documents gave me the right to act on her behalf and take care of her financial affairs. The technical term is that I became her attorney-in-fact (AIF). We had to shut down her apartment (where she fell) and moved her legal address out to my brother and sister-in-law's house. We had to deal with her cell phone provider, banks, insurance companies, the cable company, utilities, the DMV (a completely different hot mess), and more. Everyone wanted some level of proof that I was supposed to act on her behalf.

Lesson 1: Don't wait until an injury or illness to get the proper legal representation and documents in place. Had my mom been brain damaged during the fall, I would have had to go to court to be appointed her guardian, which would have been a much bigger pain to do and deal with.

My mother had numerous department store credit cards, most of which were very old. The older cards generally didn't have 16 digits on the front. Most of these were already expired accounts. However, it is necessary to call and make sure these accounts are truly dead and shut off. If they are not, then she is more likely to be the victim of identity theft. Since we had to qualify her for Medicaid (which includes spending her down to a net worth of $2000 plus a car), anything like this would be fiscally devastating, and a royal pain for me to have to fix. All the cards were chopped up.

Once I explained Mom's situation, considering that most of the accounts were already closed, they didn't ask for my POA papers. They believed me when I said that I was the AIF, and confirmed that I already had what I wanted.

Lesson 2: Get your parent's SSN number from them while they are still alive. They probably have yours so they can conduct affairs for you (especially if you're recently or currently a minor). Turnabout is fair play, and it makes it much easier to manage things in situations like this.

On the couple of occasions that department stores had valid credit cards that weren't a branded Visa or MasterCard, it took more convincing, but I was able to close the accounts. Fortunately, my mom hadn't used them in quite a while, and I was asking to close the accounts. It turned out okay.

After those cards were taken care of, there were four cards left: a Sears gold MasterCard, a pink Discover card, and two Chase credit cards (the one about to expire, and the one that had to be activated). My goal with these cards was to keep them active, get the address changed to my brother's house, change the phone number, and reactivate the Chase card.

My mother didn't have a net presence. No email, no computer, no nothing. So, my sister-in-law (who has been great about helping during this trying time) took advantage of this, but forgot to tell me. The same kind of thing happened when shutting off the cell phone with Verizon, but I digress. I was dealing with the automated system and was asked to enter Mom's full credit card number. I did so. I was then asked to enter the last four of her SSN. I did so. I was then asked to enter her zip code. I did so, using the old address. It rejected that. I tried again, and it rejected it once again. I got inspired, and entered Mom's new zip code, and it took. I was then able to get to an agent. The agent wasn't able to officially talk to me because they didn't have the POA papers on file. However, by asking the right social engineering questions, I was able to figure out that my sister-in-law already updated the address on the web. Problem solved.

Lesson 3: If more than one person is working on this, coordinate efforts. It is possible now that they realize that the address was changed online,

they may shut off the card. Let's hope not.

Lesson 4: Use technology when you can.

Then came Discover. With either mom's full SSN or the last four (can't remember which), and her mailing address, I was able to change her address and phone number strictly through the automated voice recognition system. I never had to talk to a person, and it took about 3-5 minutes tops.

Lesson 5: Close your Discover account - their security absolutely sucks.

Chase was the most important card. It had the highest credit limit, the most recent renewal, and the most penetration. Unfortunately, my mom will probably expire before the card does. It was also among the most instructive.

When I phoned, things seemed to go very well. I called them first, and I thought the whole project was going to be a breeze. Then they asked me for the POA papers. Having them scanned in, I asked where to email them. I was told they had to be faxed. I got the fax number, and then asked when they would be in the system. They told me "two hours." I was fine with that, as I had to be up that long anyway.

Lesson 6: Work within the system.

Three hours later, I called, and was directed to a supervisor, who told me that he couldn't help me. I told him that I had faxed the papers in. He told me that he saw that, and saw them, but that they had to be mailed. This wasn't acceptable to me for a few reasons. First, why would they give me a fax number if faxing the POA papers in wasn't acceptable? Second, there was no guarantee that the papers wouldn't get lost, and draw out the process. Third, we were trying to qualify my mom for Medicaid by the end of the year. Had we not done so, she would be on hook for another month of private pay at the nursing home at about $7,000 a month. Had we qualified her and not resolved the credit card situation before, she may not have been able to keep her credit. Needless to say, I was not happy, and let the supervisor know as much. I asked to speak to *his* supervisor, and was told he didn't have a supervisor.

Lesson 7: Don't believe everything that everyone tells you.

I called back the next morning, got a representative on the phone, and did with ease what I should have been able to do the night before. The POA papers were there, but I had to prove that I was the AIF. The woman figured that I should know my maternal grandmother's maiden name. I didn't. I had never thought about that, as she was dead long before I was an idea. Not having my grandmother's maiden name was a show stopper. Then, the woman on the phone gave me the hint I needed. She told me the first letter. It was the first letter of some cousins' last names. There are other places that name shows up too, but for me to say it in this magazine would open us up to identity theft, so I can't go there.

Lesson 8: Ask your mom what her mother's maiden name is.

Lesson 9: Social engineering works. The woman had pity on me to give me that hint, which opened the door.

With my grandmother's maiden name, the woman at Chase decided I was the AIF, and I was allowed to change the address, phone, and activate the new card. I also had the representative lodge a complaint against the "supervisor" that wasn't really a supervisor (see lesson 7).

So now my mom has an emergency credit bank that we can use that should last at least through the next few years.

ASAT FOR DUMBASSES: PART TWO - DETECTING AND TRACKING STEALTH SATELLITES

by spynuclear@yahoo.com

This is a continuation of "Anti-satellite (ASAT) System for Dumbasses (27:4).

This article will describe a system that can be used to detect and track a low observable (stealth) satellite. These particular birds are dedicated reconnaissance assets that scan high value targets. The stealth characteristics are incorporated to involve visible, IR (Infra-Red), and radar frequencies to evade detection. This is accomplished by using special radar absorbent paints and materials. Optical stealth is achieved by using satellite panels painted flat black. My system is designed to bypass these restrictions. Laser scanning a section of the sky and gathering the reflected light from the target satellite accomplishes this. The CCD camera feeds the signal

to a computer and uses specialized astronomical software to detect the satellite. Other software is used to convert the data gathered to predict satellite orbital data and the next overhead pass. My system uses the following:

- Meade ETX-90EC. Computerized telescope with an integral satellite tracking capability.
- Meade LPI (Lunar Planetary Imager) CCD camera. You can use any consumer grade CCD camera that records in AVI format.
- Lunarscan 1.5. Specialized astronomical software that is used to detect micro-meteorite impacts on the moon. We are going to trick the software to recognize the reflected laser light from the stealth satellite as a lunar meteor impact.
- Shortwave radio. Used to get the most accurate time signals from WWV (2.5, 5, 10, 15, 25 MHz), CHU (3330,7850, 14670 kHz). This is needed for accurate orbital elements determination of the target.
- Handheld laser barcode scanner. I use a surplus scanner unit that has been modified by adding red and green laser modules piggybacked onto the unit so that they fire into the rotating mirror assembly.
- Satellite tracking software. I use a variety of software for orbital elements tracking. I recommend that the user try various software packages such as Orbitron, SatTrack, Psat, Pocket Sat Plus, and others. See what works best for you.

The setup is to mount the modified laser barcode scanner so that it fires up in the sky. The LPI camera is mounted onto the ETX-90EC telescope. The camera takes a series of images and feeds the images to the Lunarscan software for target detection. The telescope has an option for the user to read out the aiming data to wherever the telescope is pointed at. This data with accurate location, timing information, satellite transit data, and angles will give the observer a rough set of orbital elements. Repeating this procedure over several sessions will give much more accurate orbital data. This makes tracking the stealth satellite much easier and more accurate.

The data reduction procedure from the observing session consists of getting the following data from each satellite observing pass:

- Location. GPS is best.
- Date / Time. Local date and time as well as time in Julian format or Universal Time.
- Start Azimuth Angle. The starting azimuth angle of the satellite pass above the local horizon.
- End Azimuth Angle. The ending azimuth angle of the satellite pass above the local horizon.
- Pass Time Elapsed. The time (in seconds) that the satellite is visible.

This information forms the basis for orbital element determination. This data is used to determine and generate the future orbital pass and tracking data.

Some satellites are stealthed so that they can sneak up on their targets. They are launched into orbit and moved into a new orbit as their mission tasking changes. Due to a limited fuel capacity and restrictive mission tasking requirements, this is done rarely. Some recce sats are run in "silent running" mode to look like dead hardware until needed for a mission. Some are run in an orbit that looks like an innocent communications or weather bird. These sats are activated and moved to a new orbit to sneak up on the required target. Some hunter/killer sats can be disguised anti-satellite weapons platforms for sneak attack mission profiles.

My next article in this series will concern the building and operation of a quantum gravity based mass defect sensor system. This is a passive device that detects an object simply by that object's existence without generating any emissions that can be detected. This device is specifically designed to detect and track stealth aircraft missiles and satellites. This is a type of an esoteric field called anti-stealth technology. This technology has the ability to completely render current stealth technology applications and billions of dollars of stealth aircraft, missiles, and satellites totally obsolete. It not only detects and tracks the object, but also determines the object's mass and Doppler velocity, which has an effect on the object's orbital lifetime and other characteristics.

References

- *Using the Meade ETX: 100 Objects You Can Really See with the Mighty ETX* by Mike Weasner
- *Using a Computerized Telescope* by Michael Covington
- *Observing Earth Satellites* by Desmond King-Hele
- *Methods for Orbit Determination*
- *Practical Astronomy with Your Calculator* by Peter Duffet-Smith
- *Practical Astronomy with Your Computer* by Peter Duffet-Smith
- *Easy PC Astronomy* by Peter Duffet-Smith
- *Scientific American / The Amateur Astronomer* - Shawn Carlson (editor)
- #21 - "How To Study Artificial Satellites"
- #22 - "Predicting Satellite Orbits"

Pen Testing from a Mile Away

by Asim Zaman

Are you unimpressed with your wireless card's range? Fed up with limited number of available access points? And like many other families in America, have a now unused satellite dish cluttering up your house? Constructing a Wi-Fi satellite dish can greatly extend your Wi-Fi range and open up many new interesting possibilities. During my time working as a help desk tech for an office building, I was eventually given the task of setting up their wireless network. With this came the penetration testing, to see how vulnerable they actually were. Now, here I faced the difficult task of wandering around the building trying to get in range of all the various access points due to my built-in wireless card's pathetic range, all the while jumping from power plug to power plug due to my pathetic battery. This kind of job can be tiresome and can grow into an even worse problem when dealing with larger area projects such as college campuses or corporate parks. The Wi-Fi satellite dish allows you to cover a seemingly endless range with no movement whatsoever. The potential is infinite.

When beginning this project, you are going to want to gather up six different parts. Each is essential to the operation of the satellite dish.

The Dish: Any satellite dish will do, but it helps to have the antenna (the small pronged piece that extends out and resides in the hot spot of the satellite dish). A lot of times, dish networks will take back this piece, but you may get lucky and find a complete dish. Without the antenna, you will have to manually find the best spot to position your handmade receiver, which can be accomplished by a trial and error method.

The Wi-Fi Adapter: I recommend purchasing the Alpha Network's AWUS036H. This particular Wi-Fi USB adapter is equipped with several features that are much better than other models:

1. The chipset. This make and model contains the RTL8187 chipset, which is very compatible with aircrack and backtrack. This allows it to be ideal for pen testing.

2. The power output in this model is higher than that of other USB dongles in that it was built as a long range USB adapter. It therefore is capable of even further increasing your range.

3. The SMA male connector. This particular feature is essential for connecting the Wi-Fi module to the dish. This port is the segment where the antenna would normally attach.

The Cable: This cable needs to be the SMA female to N connector cable. By searching for this on Amazon or on Google, you can find one for a minimal price. I recommend getting one of six to twelve feet in length to give you plenty of maneuverability.

The following materials are used to create the satellite antenna.

Copper Wire: Simple enough.

Copper Flashing: A little expensive but still easy to find.

The N Connector: This piece may be the most difficult to procure, but a good place to start is at a local electronics store, or again from Amazon. The official name for this is "Coaxial Connector, N Type Panel Jack (Square Mtg)"

Once all of these materials have been accumulated, the actual construction can begin. The only real construction that needs to be done is the assembling of the antenna. During this assembly you will need to solder the copper pieces to the N connector and attach the N connector to the copper flashing. This can be done in a few simple steps.

First, you must cut a length of wire measuring 244 mm in length. Then, you will mark the wire every 31 mm so that you will have eight equal segments. You will now begin to bend the wire into a series of 90 degree angles that will end up in the shape of a double diamond. To make really sharp edges, I recommend that you use two pairs of pliers held perpendicular to each other. This way, when they are twisted against each other, you get a very sharp 90 degree angle. The best way to complete the double diamond is to bend it into two equal squares.

The next section is building the mounding element. First, cut out a 110 mm square of black plastic and drill a hole in the center wide enough for the white piece of the N connector to clear. Now you need to solder the copper wire to the N connector. You should fit two pieces of copper wire (length does not matter - they will be cut later anyway) and solder them at two points. The first wire should be directly fitted into the N connector's gold pin and soldered there. The other wire should be connected just outside the lowest metal ring on the metal panel itself. I recommend you use a

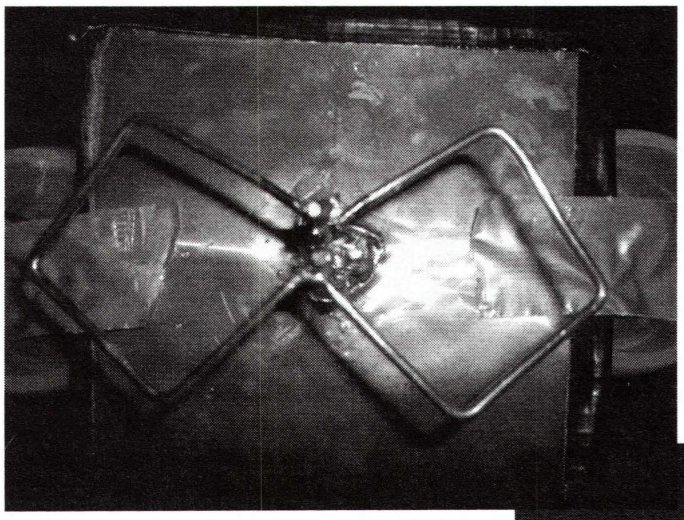
propane or butane torch for this part, as a soldering iron does not produce the heat necessary to bond the metals.

After the connector is cooled, attach it to the black plastic base using an epoxy. The copper flashing should be attached to the front and trimmed to fit, also with a hole drilled to allow the N connector to pass through.

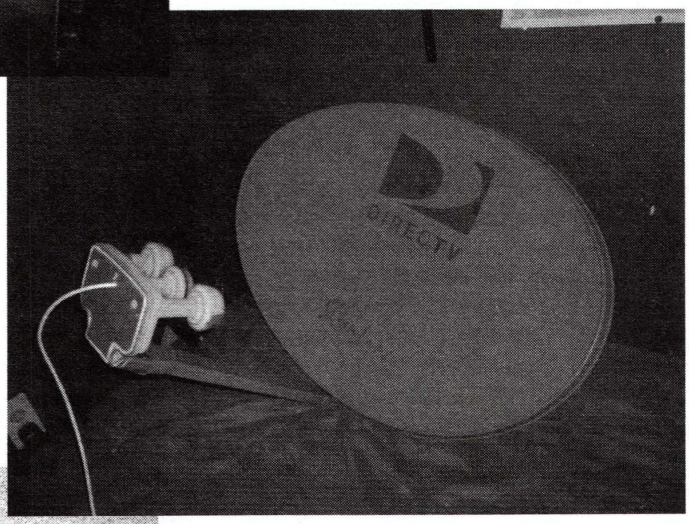
The next step is to solder your bow tie shaped element to the vertical wires. I recommend you use two pieces of scrap copper flashing, 15 mm wide to support the double diamond so the height is even on both sides. Then it is the simple task of soldering the wires together.

Next was the task of mounting and attaching the antenna to the dish's antenna. Each satellite antenna differs with make and model but essentially you must remove all the plastic covering pieces so that the receiver's hole is apparent. Then you must feed the wire through this hole and connect it to the antenna and to the Wi-Fi module. Once this is complete, you are ready for action.

My usage of this module was for penetration testing and that is how I tested this dish's effectiveness. I used the airodump-ng program on my Backtrack 4 Final Virtual Machine and was able to receive a much greater range of Wi-Fi access points. Before, with just the bare module, I would pick up approximately four or five points in my target area. But after I put the dish online, the amount of access points refreshed off the end of my monitor.



Completed antenna module



Completed Satellite Dish

Wireless module

Securing Online Voting

by kr

Introduction

I work as a programmer in a large company (based in one of the European countries) that provides web support for various online campaigns for big domestic and international companies. We prepare more or less complicated websites, Facebook applications, online forms, etc.

Lately, I got a few assignments to prepare websites for competitions, i.e., an Internet user uploads some image, photo, etc., which is then rated by other people. The entry with the most votes wins, plain and simple. In this article, I will share with you some of my experience on securing (and hacking) such applications.

There are many methods to secure voting applications. None are perfect. Here's a short list. (I didn't elaborate on some of the methods, as you may be familiar with them. If not, visit the websites referred to or Google it.)

Overview of Methods

1. *Cookies* - the simplest method (to implement and to evade). In short, you, as a developer, can save a small text file on the user's computer and read its contents later (at least, if the user is not a paranoiac freak who turned cookies off). Evading cookies is as simple as turning them off, deleting them, or changing their contents. This works for some less experienced cheaters. Recently (September/October 2010), some smart guy developed "evercookies" (`http://samy.pl/evercookie/`), an API that tries many different methods of storing the "undeletable" equivalent of cookies. It's nice, but it doesn't work when you are connecting in a different method, like Curl, or using the "safe" mode in your browser.

2. *CAPTCHA* - this acronym stands for "Completely Automated Public Turing test to tell Computers and Humans Apart." In other words, it's more or less garbled text displayed to you that you have to retype. In many situations, it'll help you to avoid people who would like to write automated scripts to do the dirty work, although if your CAPTCHA is lousy, it is easy to read it with some OCR-like script. If it isn't, there are some Russian folks who would be happy to help you (`http://captchabot.com/en/index➥.html` - I didn't test them and am not endorsing them in any way; I'm just impressed by their service, and maybe you'll find it useful). It's still not effective against folks who sit at their computer 24/7 and press "vote" every five seconds and then retype the password (more about that later).

3. *Email Confirmation Link* - the vote would be counted only when the user clicks on the link that is sent to him/her by email. The main advantage of this method is that the process is more time consuming for the user (so it's a little bit harder to mass vote). Filtering out illegitimate votes is possible, but needs some knowledge from the perspective of the attacker. You can block known disposable email addresses like spam.la or 10minutemail.com; you can see if someone tries to use known capabilities of free mail services (i.e., in Gmail, those addresses are connected to the same account: `example+something➥@gmail.com`, `e.xample@gmail.com`, `e.x.a.mple@gmail.com`, etc.); other evasions can be tracked in the post analysis, i.e., you can see that somebody created a catch-all alias in their own domain, or is using free addresses like `john01@yahoo.com`, `john02@yahoo➥.com`, `john03@yahoo.com`, etc.). A more annoying extension to this method is forcing users to register an account on your site.

4. *Facebook Connect* - it's not always a good idea, but sometimes the competition is directed to the Facebook users. The Facebook user ID is an additional variable that we can take into account (but it is not wise to rely only on that!).

5. *IP Limit* - limiting one vote per IP (i.e., per day). It looks like the best idea, but isn't always. For example, ADSL or mobile providers don't assign their subscribers a fixed IP. Instead, they can change it every time a connection is established. A Tor network (`http://www.torproject.org/`) might be used to change one's IP address every time they wanted. On the other hand, people in the same network (office, home, or university network) would be unable to vote, even if they were on different workstations, as they are visible on the outside as if they were connecting from the same host.

6. *Browser Fingerprint* - nice method that you can read about at `https://panopticlick➥.eff.org/` and `http://www.network➥world.com/news/2010/051810-eff-➥forget-cookies-your-browser➥.html`. It turns out that your browser leaves many traces that, combined into one, allows for a quite unique fingerprint. As with evercookies, it's good for non-advanced users using browsers, but completely useless if someone wants to cheat you using Curl or something.

7. *SMS Verification* - OK, in my opinion this method is the best, but clients don't want to implement it because it's expensive. The idea is simple

- if you want to vote, you have to give your mobile number. We send you an SMS with some code that you have to use to validate your vote. The rule is that you can only place one vote per mobile number (i.e., per day, week, or just one and only one). It's highly unlikely that someone will have many different mobile numbers at his/her disposal.

As you can see, none of the methods is perfect in itself (maybe the seventh is). My suggestion is to combine some of them and then, as a last resort, add some techniques of analyzing votes after they have been placed. More on this later.

Case Study

As an illustration of the problem, I'll share with you one of the cases. It was a project for some big international company, which I will not identify to protect their (and my) business. The idea for the competition was quite simple - people would upload images on the given subject, and then visitors could vote for the photos they liked most. The winner would be given quite an expensive prize, worth an equivalent of $3500 or so. In other words, the stakes were high. So was the number of people wishing to cheat.

I presented the customer with some recommendations based on the list above. Unfortunately, they decided to employ the least effective and most vulnerable techniques: protecting by CAPTCHA, cookies, and IP limit. They didn't want to employ any demanding or expensive methods. So that was it. I had no choice.

So there it was on the production server - my application (that I was not so proud about) with weak protection, waiting for some rascals.

It wasn't a big surprise to me when, a day or two after the competition was announced, some of the entries started to gain more votes than the others. At this point, the battle began. First, I exported a list of votes per image with their times and IPs. I ran blocks of IPs through the databases (available online at `www.ripe.net` (Europe), `www.arin.net` (North America), `www.apnic.net` (Asia and Pacific), `www.lacnic.net` (Latin America and Caribbean), and `www.afrinic.net` (Africa)) to get ISP information for the votes. It turned out that cheaters were using ADSL or mobile wireless connections that allowed them to change their IP when they reset their modem. I concluded that they were still typing in the CAPTCHAs manually because the interval between consecutive votes was significant, as well as (which I found quite funny) the fact that voting started at around 8 to 10 am (when they woke up) and ended around 11 pm to 1 am (when they went to bed). To prevent those guys from voting, I just blocked some IP ranges. I observed that legitimate voters weren't using mobile networks to vote anyway.

This action caused a big decrease in the illegal votes. But, a few days later, I noticed some other guy doing funny stuff. The pattern was the same - lots of votes placed all day with a break for sleep in the night hours. One thing was different. IPs were changing all the time, but they weren't from the same network. They were from all around the world! Germany, then USA, then Japan, China, some African countries, and so on. I quickly realized that this guy was using Tor or some similar network. Fortunately, the rules of the competition were saying that only people in my country were eligible to vote and win. So I found a database that provided information about the country of origin of every single IP address (Google for "IP geolocation free"). Two hours later, every vote from abroad, past and future, was invalid.

In the meantime, I added some more security to the site, making "cookies enabled" a requirement and adding some session variables loaded on the page showing the photo (just before the vote). It allowed me to cut some of the less experienced cheaters.

For a while I thought that it was over. But I was wrong. There was still one guy voting all the time. He was using a trick with changing IPs all the time and I wasn't allowed to ban his IP range because it was the most popular ADSL provider in my country (ten percent market share). One thing that I noticed was that he was voting all the time, even in the night. It was impossible for a living person to do this, so I concluded that he had some script to pass my (lousy) CAPTCHA. The cure was simple. I found an open source script with some more sophisticated, distorted CAPTCHAs and implemented it. It turned out his skills were not enough to crack it and he was too lazy to type every CAPTCHA for 12 hours a day.

Finally, I won. It all ended happily. The grand prize was won by a recently married couple who posted their sweet photo everywhere online and asked people to vote. One thing that I found significant about this and others' legitimate projects was that, when analyzing sources of their votes (IP blocks), it turned out that they were spread evenly and over a large number of different networks (hundreds of different networks), while votes for cheaters' projects were coming in large quantities from only a few networks.

Conclusion

OK, so what's the conclusion of this story? Sometimes, you have limited resources and you can't apply sophisticated techniques to protect your application, but looking into the logs and trying to get into the bad guys' minds can help you to defeat the evil (of course you can "look" into logs in some automated way - that is something I plan to work on, having new experience from these projects).

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! It's been an interesting few months. Things have settled down into a reasonable rhythm in bringing our new Central Office online and, with the project schedule on track, I've been able to enjoy a little personal travel around Asia. My most recent trip was to the DMZ, one of the world's most dangerous places.

In 2005, I was one of the first Americans to visit the DMZ from the north as a tourist, so it was interesting to see it from the southern side a few years later. The experience visiting from the north or south is largely the same, each side detailing a litany of grievances that have not been resolved in nearly two generations, showing off weapons seized from the other side, and claiming their soldiers will protect you from the opposite side's aggressions. The two Koreas are like perpetually quarrelling siblings, with long-held grudges over disagreements that ceased to really matter decades ago but are still unforgotten, each side staring at the other over the world's biggest spite fence. The only difference is that an angry shouting match has the very real possibility of escalating into World War III. This is, presumably, why Bill Clinton called the DMZ "the scariest place on earth."

Despite being technically still at war, separated from North Korea by an uneasy armistice and thousands of troops, South Korea is an incredibly modern society. On my last visit to Japan, I found myself wondering where all of the new technology went. Having visited Seoul, the answer is obvious: Korea. It's not often anymore that I find myself completely marveling at technology that I've never seen before, but in South Korea you'll find that this is commonplace. From enormous displays at bus stops that provide multi-touch enabled satellite maps you can use for trip planning to ultramodern mobile phones, Korean society is at the leading edge of technology.

This is particularly evident in telecommunications, nowhere more evidenced than mobile phones. Like Japan, South Korea doesn't support GSM. Only flavors of CDMA are supported, both WCDMA (which many AT&T and T-Mobile USA world phones support) and 1xRTT/1xEV-DO (used by Sprint, Verizon, and US Cellular in the U.S.). If you carry a GSM-only phone, you can rent an unlocked WCDMA-capable handset at the airport for about $3 per day (plus a hefty deposit), and if your carrier allows you to roam on a South Korean carrier, you can simply insert your home SIM card. Strangely enough, though, I couldn't find a local SIM card for sale to use in my WCDMA-capable HTC phone. You can only buy one along with a prepaid mobile phone. Foreigners are only able to buy prepaid handsets, and are not allowed a monthly subscription.

I carry a WCDMA-capable handset and my Chinese carrier has a roaming agreement with both SK Telecom and Korea Telecom, so roaming was seamless and surprisingly cheap. Outgoing calls within South Korea cost less than 10 cents per minute, with incoming calls costing about double that (owing to the charge for delivering the calls long distance from China to South Korea). Data roaming was still expensive, at a rate of about $1.50 per megabyte, and text messages cost about 10 cents each. All features worked seamlessly, and Chinese government restrictions on accessing certain websites were enforced. When roaming in Korea with a Chinese phone, your data is still forwarded through a gateway in China, so your mobile web browsing is subject to Chinese laws and regulations.

North Korea uses a GSM system, but a side effect of the jammers used to block radio and television signals coming from South Korea is blocking of mobile phone signals from the north. Technically, South Korean WCDMA handsets are backwards compatible, but cannot roam on the system. In North Korea,

WCDMA and CDMA-capable handsets are not available which effectively prevents any attempts to use the South Korean system (and presumably, North Korean users won't be allowed to roam anyway).

Unlike in Japan, smartphones have made tremendous headway in Korea. They are tremendously popular; most people I saw with a mobile phone across two visits to Seoul were carrying one. Approximately 60 percent of smartphones are powered by Android, according to KCC (the Korean equivalent of the FCC) statistics. Local brands Samsung and LG are the most popular, probably due to their superior Korean-language support and localized features. As in many countries, local search and application providers have the most popular applications, with Naver (a local ISP and online services provider) leading the pack. Google, however, is making headway with its search engine on mobile phones (although not on traditional browsers), largely owing to its integration with the Android platform. So is Facebook, although like Google, it seems more popular on mobile phones than on PC browsers. One smartphone platform that is practically missing - as in Japan - is the iPhone. You do see people with iPhones, but they are more expensive and less popular than the heavily localized Korean brands.

Despite the adoption of smartphones with high-resolution cameras, QR codes seem not to have caught on at all. You see them everywhere in Japan, and they are growing in popularity in more developed parts of China. However, I only saw one QR code across two visits to South Korea, and it was on a Korean Airlines boarding pass. This is somewhat surprising, given the low cost, high quality, and high speed of data services in Korea. Downloads run at 2Mbps and with WCDMA, you can download your email and make a phone call at the same time. This is important, because Koreans, unlike Japanese, make relatively more phone calls and send relatively fewer text messages.

One particularly interesting - and growing - area of mobile telephony in South Korea is mobile payments. SK Telecom has run a proprietary system for the past few years, but there are only limited places you can pay. Recently, they made an agreement with Japanese carriers KDDI and Softbank to develop and roll out a system called NFC. This system is based on an RFID-enabled SIM card, which broadcasts at 13.56MHz. The billing platform is developed by Visa, and is called PayWave. This allows up to eight credit cards to be linked to a single mobile phone account. Additionally, the platform allows for the application that nobody seems to want but never seems to go away - mobile coupons. Your carrier can use your GPS coordinates to send you coupon spam, and these can be stored on your NFC SIM to be presented wirelessly at merchants along with your payment credentials. Providers are very tightlipped about the technology and there is very little published research on the platform, but they have publicly stated that it is based on "ISO7816 or 14443 standards." The SK Telecom system is branded "T-Smart Pay." Time will show just how smart it is.

Innovation in telecommunications is not limited to wireless phones. Internet service in South Korea is based on fiber to the home, and runs at speeds exceeding 40Mbps. It's incredibly fast, very inexpensive, and South Korea leads the world in broadband penetration with over 70 percent of homes subscribing. Of course, you can also still use a payphone if you want to. These are located nearly everywhere in quantities far exceeding the U.S. Most take cards, some take coins and cards, and many new phones (yes, I said new payphones - South Korea is still innovating here) allow paying with a T-Money card. T-Money is a prepaid RFID payments card operated by the local transit authority. In addition to payphones, subways, and buses, you can also pay for taxis and even pay for items at many retailers with the T-Money card. Oh, and did I mention the technology platform? The whole system runs on the infamous Mifare Classic RFID platform. Is T-Smart Pay built for easy integration? I don't know, but RFID hackers may find this an interesting question.

And with that, it's time to draw this issue of "The Telecom Informer" to a close. Have a safe summer, and I'll see you at Photosynthesis Festival and Def Con 19!

Mobile Hacking with Android

by MS3FGX
MS3FGX@gmail.com

If you have been following the mobile industry for the last year or so, you have already heard about Android. Google's mobile Linux operating system has taken the industry by storm, and analysts predict that by the end of 2011, it will have overtaken Apple's iOS as the number two mobile operating system in the world. Some even say that by 2015, it should overtake Nokia's Symbian OS as the number one mobile OS.

The continued success of Android is of particular importance to hackers, as it is more proof that a large scale open source project can not only compete with proprietary software, but excel beyond it if properly supported. Perhaps more importantly, the open nature of Android allows its more technically inclined users to peer into the workings of their mobile devices and modify them however they wish. Finally, the dream of an open mobile device that started with the OpenMoko FreeRunner is very close to realization for the mass market.

Of course, we know that every story has two sides. With increased hardware performance, storage capacity, and software capability, mobile devices have become increasingly tantalizing targets for attackers and criminals over the last few years. But with flexible operating systems like Android under the hood, mobile devices are now becoming practical attack platforms, allowing an attacker to scan for and engage targets from the palm of his hand.

This article will take a look at a few Android applications of interest to both the hacker and the criminal alike, and detail a proof of concept attack using nothing more than a rooted Android mobile phone and publicly available software. The information herein is provided entirely for educational purposes so that the reader may have a better understanding of the capabilities and realistic applications of this technology. It in no way condones or suggests attempting to use these techniques in a malicious manner.

What is Android?

To get a better understanding of what Android is capable of, we should first get a good handle on what it actually is.

In 2005, Google acquired a little known company called "Android, Inc.", which had been developing software for mobile phones. Soon after, Google began filing various patents with a focus on mobile phone technology. This prompted the media to begin speculating that Google was planning on releasing a "G-Phone" to go head-to-head with Apple's immensely popular (and largely unchallenged) iPhone.

But in 2007, rather than announcing a single phone they intended to bring to market, Google brought together a group of some of the most important companies in the mobile industry and created the Open Handset Alliance (OHA), a consortium designed to develop open standards for mobile devices. The OHA revealed that their first product would be an open source mobile OS called Android, designed to run on the full gambit of mobile devices (phones, tablets, netbooks, etc.), rather than an OS tied to a specific piece of hardware (like Apple's iOS). In October of 2008, the HTC Dream (more commonly referred to as the G1) was released and became the first official Android device.

Android is made up of several software layers which are intended to make the OS more modular and easier to develop for. Android is based on the 2.6.x Linux kernel which handles hardware interaction, GNU userspace utilities for low-level system management, and various open source libraries such as OpenGL, SQLite, and FreeType.

While this technically makes Android a GNU/Linux OS, Android applications (or "apps" as they are usually referred to) are not native Linux binaries. Rather, Google has developed a Java virtual machine called Dalvik and a large framework of libraries which developers can use without ever touching the underlying Linux system. This means that developing for Android requires no previous knowledge of Linux programming, and allows the developer to work within a well documented and defined environment, regardless of what device their code will eventually run on.

The idea that a developer should be able to write one application and be able to deploy it on essentially every piece of hardware Android itself supports is a core element of the OHA. In theory, this should be a boon for developers, but in practice, it introduces a number of problems, one of which being that Android applications are never truly optimized for a specific device, and are always limited by the capabilities of the Dalvik VM. Updates to Dalvik and the introduction of the Native Development Kit (NDK), which allows

developers to bundle in native C code with their Java applications, are beginning to alleviate the issue, but hardware intensive applications like 3D games are still noticeably absent from Android's software library.

While not a viable option for large-scale Android development, it is also possible to write (or adapt) Linux C code for use with Android. In theory, this means you could take existing Linux tools and applications and cross-compile them for the ARM architecture most Android devices are running on. In practice however, there are a number of limitations imposed by the abridged nature of Android's Linux implementation that make things more difficult. Most notably, Android doesn't include libc, but rather uses its own library known as Bionic. All native Linux code must be compiled against Bionic, but as Bionic is not 100 percent compatible with libc, there is no guarantee that code will work as expected (or at all). In addition, Android doesn't use an X server, so graphical Linux applications are out of the question.

As with all UNIX-like operating systems, Android has a very strict set of permissions, which in this case extend from the core Linux components all the way up to the Dalvik VM. Since anyone can write an Android application and publish it in the Android Marketplace, it is extremely important for the system to monitor and limit the capabilities of everything the user installs. Every application must list its capabilities in regards to the Dalvik VM for the user upon installation, and Linux's standard per-user filesystem permissions prevent even rogue applications from accessing the underlying OS and doing system-wide damage.

While that is fine for the average user, those of us who want more control over our systems can start to feel a little caged in. Just like in a full Linux OS, if you want to get complete access to the system, you need to elevate your user level to root. Gaining root privileges is not technically supported by Android, and doing so usually requires making use of some exploit or glitch in that particular device's build of Android. Accordingly, the process of "rooting" an Android device differs greatly depending on the hardware and what version of Android it's running, which makes it considerably out of the scope of this particular article. I can say that, as far as I am aware, all Android devices currently on the market can be rooted, with varying degrees of difficulty or Linux knowledge required. A simple Google search of your device name along with the term "rooting" should get you started.

Android Software

Even though Android has been on the market since 2008, it wasn't until relatively recently that it started to take off. Android's surge in popularity (at least in the U.S.) is considered to be due in large part to Verizon Wireless and their DROID lineup of phones, specifically the Motorola Droid, which more or less became the de facto Android 2.0 handset. With an increased userbase comes more developers, and as such, Android software has started to mature and offer legitimate tools and applications rather than the drivel that populated the Android Marketplace for the first couple of years of the OS's life.

At the same time, Google's release of the NDK and the fact that Google doesn't prevent or discourage rooting Android has led to some very powerful and useful software that anyone can install and run without fear of persecution from Google or their device's manufacturer.

In the following sections, I will briefly go over some applications of particular interest to the hacker. All of these applications are available on any Android device that has access to the Android Marketplace, though some do require your device to be rooted as mentioned in the previous section.

WiFi Analyzer

WiFi Analyzer is one of the most popular applications in the Android Marketplace, which is really a testament to how wildly useful this tool is for both the average user and the more technically inclined. In the most basic of terms, WiFi Analyzer is a tool to scan the area for Wi-Fi networks and determine which channel is the least populated so you can adjust your own hardware to a less congested part of the spectrum.

But as the application has evolved, it has picked up a number of other helpful features. For every detected network, it offers multiple detailed graphs of signal strength (strength over time, comparison to other networks in the area, etc.), MAC address, and encryption used. There is even a function where you can lock onto a specific network and view the signal strength as an analog gauge, complete with an audio tone which increases in frequency as the signal gets stronger; an absolutely invaluable tool for locating Wi-Fi devices in the field.

That said, it is important to realize that WiFi Analyzer is *not* a full fledged Wi-Fi scanner or "wardriving" tool. As of this writing, there is no method to export the list of detected networks to file, and some functions (like the signal strength versus time graph) won't even retain their data when switching to one of the application's other modes.

ConnectBot

ConnectBot is an exceptionally well done SSH/Telnet client, which also acts as a terminal emulator for the local Linux sub-system. While there are better terminal emulators (though not for free), there is no question that ConnectBot is the absolute best SSH client available for Android.

In addition, ConnectBot also allows you to

set up SSH port forwarding from your device to a remote server, otherwise known as SSH tunneling, a topic that has been covered numerous times on these pages. Tunneling is an exceptionally useful technique for circumventing firewalls or protecting your data on public networks, both of which are very useful on mobile devices. The SSH forwarding in ConnectBot is not quite as polished as I would like, such as needing to keep an interactive shell open when using the tunnel instead of doing it in the background, but it works well enough.

Network Discovery

Network Discovery is a handy tool for finding and enumerating devices on public Wi-Fi networks. Network Discovery uses a simple ping scan to find hosts on the network, and then allows the user to select one of the found hosts to target for a TCP connect() scan.

The execution is pretty basic, but Network Discovery does have a few nice touches such as a NIC vendor database, which shows who manufactured the network interface of the discovered devices, service detection (by reading the service banner), and the ability to directly connect to services which Android supports or has known applications for (WWW, FTP, SSH, etc.). Future plans include database storage for scan results, OS fingerprinting, NAT traversal, and root-enabled functions like SYN scans.

Wireless Tether

Wireless Tether is a mainstay of rooted Android phones, as it allows any Android phone to share its cellular Internet connection out over either Ad-Hoc Wi-Fi or Bluetooth PAN. It does this in such a way that prevents your carrier from differentiating between the traffic generated from the Android device itself and any devices connected to it, the upside being that you are able to share the cellular Internet access you already pay (dearly) for without having to sign up for the nonsensical "tethering" charges which many carriers have begun implementing. This is an excellent tool for setting up temporary Internet access for small groups of people, such as at hackerspaces or *2600* meetings.

Shark for Root

Shark for Root is a port and front-end for the venerable tcpdump. I suspect the use and function of tcpdump is well known enough that I don't need to go into explicit detail, but, to put it briefly, it allows the user to examine and log all of the TCP/IP packets going into and out of the Linux kernel. As the name implies, Shark only works properly if it is run as the root user, which allows it complete access over the kernel's networking subsystems.

Shark isn't much to look at, and, in fact, has a few rather annoying bugs in the user interface, but the UI itself is the last thing you are going to be worried about. Installing Shark is the easiest way to get a working tcpdump binary installed on an Android device (though some custom ROMs do include it out of the box), so it's an absolute must-have if you want to do any kind of mobile network analysis.]

Remote Exploit Applications

This is more of an "honorable mention" category; there are currently a handful of applications in the Android Market which are designed to use documented remote exploits against various operating systems and server applications. For example, there are a few applications designed to use the recent Windows Vista and Windows 7 remote SMB exploit. These applications can be used to trigger a BSOD on any unpatched Windows system on the same Wi-Fi network as the Android device.

While this type of software is still fairly rare on Android, it is going to become more common as developers get better acquainted with the intricacies of making software for Android. This area of development certainly warrants a close watch from the community, both offensively and defensively.

Mobile MITM Attack

So we have covered a few very useful tools you can download on your Android device, but you still might be wondering how these seemingly innocuous applications could possibly be used maliciously. A powerful mobile device running Android could be used by an attacker in thousands of different ways, but, for this example, we will be focusing on a specific case that involves a few of the applications we just discussed; using a rooted Android phone as part of a man-in-the-middle attack.

The idea is really rather simple. We will be setting up Wireless Tether to make our phone appear to be a public Wi-Fi AP (access point) to our victims, and then, once they connect to our phone (and through it, the Internet), we can capture their traffic for later analysis and data retrieval.

The first step is to scout out a good location. Tools like WiFi Analyzer are helpful here as they can be used to find important information about the existing Wi-Fi coverage in the area. Ideally, the best place to attempt an attack like this would be locations with a high density of users, and a relatively low number of existing Wi-Fi APs. Once an attacker finds a location where there are many potential targets, he can use WiFi Analyzer to determine the signal strength of surrounding APs and how many of them are currently running open networks. If there are many strong and free APs in the area, the attack will be less likely to work, but

if the only APs with strong signal are encrypted, users will be much more likely to connect to the attacker's open AP with excellent signal strength. Therefore, areas such as coffee shops and hotels would be particularly good candidates for this sort of attack as the users in the building will quickly jump at the chance for free Wi-Fi when presented with the paid access model the business is likely running.

Once a location has been selected, Wireless Tether needs to be configured to appear as an innocent public AP. The SSID can be changed from within Wireless Tether by pressing the Menu key, selecting "Setup", then scrolling down to "Change SSID". Wireless Tether doesn't allow spaces in SSID names, and also has an unusually short character limit, but in practice you can still get the point across. Changing the SSID to something like "free_wifi" should get the desired results, but for added effect it could be more contextually relevant to the target location, such as "hilton_wifi". With the SSID set as something sufficiently approachable, start Wireless Tether by pressing the large icon in the center of the screen (Wireless Tether must be running to complete the next steps).

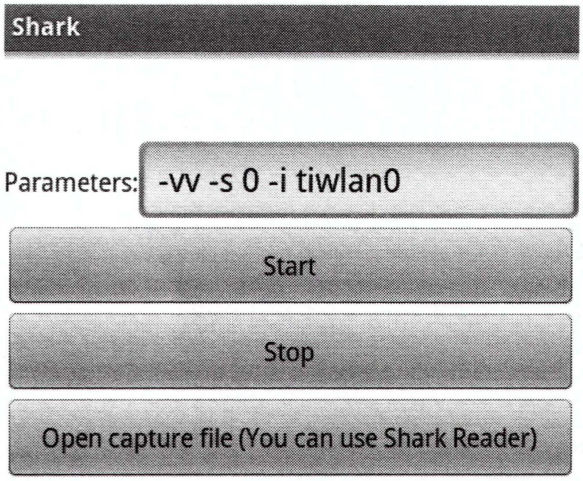
With Wireless Tether up and running, the next step would be to get Shark set up and begin logging packets. Normally, tcpdump will listen on the default interface, which in the case of a phone would be the 3G radio. Capturing packets from 3G is just going to get us a big log file of gibberish, so Shark needs to be set up so that it runs tcpdump against the phone's Wi-Fi interface where the victims will be connecting.

To do that, you need to figure out what the Wi-Fi interface is actually called. Just like on desktop Linux, some Wi-Fi drivers rename the interface instead of leaving it as the standard wlan0, so you need to do a little digging to figure out what your particular phone is running. The easiest way to do this is by using a terminal emulator (such as ConnectBot) and running the command "netcfg", which will list the device's networking interfaces like so:

```
# netcfg
lo UP 127.0.0.1 255.0.0.0
➥ 0x00000049
dummy0 DOWN 0.0.0.0 0.0.0.0
➥ 0x00000082
usb0 DOWN 0.0.0.0 0.0.0.0
➥ 0x00001002
ppp0 UP 75.206.123.22
➥ 255.255.255.255 0x000010d1
tiwlan0 UP 192.168.2.254
➥ 255.255.255.0 0x00001043
```

Here we can see the two important interfaces, ppp0, which is the 3G Internet connection, and the tiwlan0 interface, which is running Wireless Tether. You can tell them apart easily as one is running a public IP (ppp0), and the other is using a private IP (tiwlan0). The Wi-Fi interface in this case is called tiwlan because the phone in question is using a Texas Instruments chipset. Different devices will be running different hardware, so don't be surprised if you see something completely different.

With the Wi-Fi interface name in hand, you can start up Shark and add in the proper tcpdump parameters. To specify a different interface from the default, you use the "-i" option, so add "-i tiwlan0" to the parameters already listed in Shark (substituting your particular Wi-Fi device name, if necessary). Then press "Start", and make sure it begins logging packets. You should see a line at the bottom that says "Got xx", where "xx" is the numbers of packets currently captured.



Now, all that is left to do is wait. With patience and a little luck, a client device should connect to the phone and attempt to get online. Wireless Tether can be set up with various notifications when new devices connect, including a vibrate option that would let the attacker know a client has connected without making a sound or even having to glance at the phone. Once a client device connects, they will be routed to the Internet just as they expected. Their experience will be identical to that of a regular public Wi-Fi connection, and they would have no reason to suspect anything is wrong.

Obviously, there are some constraints due to the device's relatively limited processing power and bandwidth, but as long as you keep your expectations reasonable (such as using Wireless Tether's access control options to limit yourself to two or three simultaneous connections), the illusion will hold together well enough for the victims.

Once you feel you have captured enough data, simply stop Shark and shutdown Wireless Tether. You can then open up the PCAP file that was created under /sdcard in Shark Reader (a basic PCAP analyzer created as a companion for Shark),

or better yet, pull the file off of the phone's SD card and open it up in Wireshark. Assuming everything went according to plan, you should be looking at a complete log of everything your victim(s) did while connected to your "free" Wi-Fi AP.

A Step Further: Data Siphon

Being able to log all of the plain text traffic to and from the victim's computer is certainly bad, but there are limitations to the Android platform that keep the attack from moving much beyond that. As flexible and widely supported as it is, Android still only has a fraction of the tools available for x86 operating systems. Even if more advanced tools were available for Android, the processing and storage limitations of mobile devices would make it difficult to do much in the way of real-time data manipulation while still delivering the content fast enough to keep the victim from suspecting anything.

But what if, rather than attempting to manipulate the data stream on the mobile device itself, he simply redirected all of the traffic from his rogue AP to another network of which he had full control over; a network which housed machines with the software and processing capability to manipulate the victim's data in real-time? As it turns out, it only takes a few more steps to adapt the man-in-the-middle setup from the previous example into a "siphon," which can redirect all of the traffic on the rogue AP to any network the attacker wishes.

The first step is to bridge the connection between the Android device and the destination network by way of a VPN. Android comes with support for various types of VPNs out of the box, but there are some long-standing bugs in its implementation that make it all but useless in many software configurations. Luckily, the community rose to the challenge and ported over OpenVPN, which offers incredible amounts of customization and capability. Some custom Android ROMs include OpenVPN, but if yours doesn't, you can download it from the Marketplace by way of the OpenVPN Installer application by Friedrich Schaeuffelhut. The same developer also put out an application called OpenVPN Settings, which aims to make configuring and managing OpenVPN connections as easy as the built-in VPN functions, which you may also want to grab.

The actual configuration of an OpenVPN server is outside the scope of this article, but the general idea is that you set up an Internet-facing server in bridge mode. This will let you connect your VPN client (the Android device) to the server from a remote location and give it an IP that is within the subnet of the destination network. I personally used a Linksys WRT56GL running DD-WRT as my OpenVPN server, but any other implementation will work just as well.

With OpenVPN correctly configured on both sides, and Wireless Tether running, the output of "netcfg" should now look something like this:

```
# netcfg
lo UP 127.0.0.1 255.0.0.0
➥ 0x00000049
dummy0 DOWN 0.0.0.0 0.0.0.0
➥ 0x00000082
usb0 DOWN 0.0.0.0 0.0.0.0
➥ 0x00001002
tap0 UP 192.168.1.50
➥ 255.255.255.0 0x00001043
ppp0 UP 75.206.123.22
➥ 255.255.255.255 0x000010d1
tiwlan0 UP 192.168.2.254
➥ 255.255.255.0 0x0000104
```

Notice the addition of the "tap0" interface, with an IP address in the middle of the WRT54G's 192.168.1.x network. The Android device is now connected to three separate networks simultaneously: the primary 3G Internet connection on ppp0, the rogue AP running on tiwlan0, and now the VPN on tap0.

The goal now is to get traffic from our rogue AP on tiwlan0 to go through the VPN, rather than straight through 3G to the Internet. If we run a traceroute from the Android device now, we will see this is currently not the case:

```
# traceroute 75.206.123.22
traceroute to 75.206.123.22
➥ (75.206.123.22), 30 hops
➥ max, 38 byte packets
1 66.174.112.129 (66.174.112.129)
➥ 143.097 ms 75.959 ms 70.312 ms
2 66.174.112.127 (66.174.112.127)
➥ 62.164 ms 85.510 ms 69.916 ms
...
```

So what we need to do now is set up a new default route that will take all traffic out through the 192.168.1.x network's primary router (in this case, 192.168.1.1). To do this, you will use the "route" command:

```
# route add default gw
➥ 192.168.1.1 dev tap0
```

Note that, unlike the desktop Linux equivalent, the Android "route" command requires you give it an interface name.

Re-running the traceroute command from before, we can see that the path packets are taking through the phone has changed:

```
# traceroute 75.206.123.22
traceroute to 75.206.123.22
➥ (75.206.123.22), 30 hops
➥ max, 38 byte packets
1 192.168.1.50 (192.168.1.50)
➥ 300.831 ms 365.326 ms 265.656 ms
2 66.174.112.127 (66.174.112.127)
➥ 257.843 ms 257.507 ms 265.930 ms
...
```

The first hop is now the tap0 interface, so we can see that data is traveling through the 192.168.1.x network to get to the Internet, rather than directly out 3G. The keen eye will also note

the increased travel time, as data now has to run through the VPN before it gets out to the Internet. Though it is worth noting that the travel times shown here are rather high because my phone had poor signal when I ran this particular test, in ideal conditions, performance over the VPN is not much different than 3G alone.

With the victim's data now traveling through the attacker's personal network, there is no limit to what he can do. A server on the network could provide the victim's spoofed DNS entries and forged login pages, or sslstrip could be used to hijack HTTPS connections and get their plain-text content. A combination of these techniques could be used to present the victim with a convincing looking "Critical Update" page that instructs the user to "Download and install the following important system update..." before allowing them to continue on to the Internet at large.

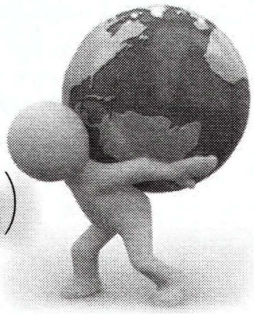
Conclusion

For those of us interested in technical exploration, Android offers nearly unlimited possibilities. Not only can an Android device be used to explore and examine the world around us, we are even given the freedom to explore and modify Android itself by virtue of its open nature. While the installation and use of security related tools on a mobile device is certainly nothing new, older devices primarily used close source proprietary operating systems the user had no control over. Even in the few previous mobile devices that actually shipped with an open source OS, you were still limited by the relative rarity of supported devices and the small userbase. The fact that you can walk into the store of essentially every cellular carrier in the U.S. and purchase a handset that runs an open source OS with development tools baked right in is completely without precedent.

Of course, the same opportunity is available for criminals, and if Android continues its meteoric rise in popularity as analysts predict, it won't be long until they start getting on the Android bandwagon too. Whether it is to develop malicious applications or remote exploits (at the time of this writing, proof of concepts exist in both cases), criminals will attempt to exploit Android's open nature for their own gains.

For hackers, Android represents not only an excellent platform for personal use and an ideal worthy of our support, but also a future battleground. As smartphones approach the ubiquity that was once reserved for wristwatches, mobile security research and development will be key in protecting users' data and privacy. The hacker ethics of exploration, experimentation, and dissemination of knowledge can aid in Android's evolution just as they once helped shape the telephone itself.

How I Escaped Google (and other web based services)



by mrcaffeine
mrcaffeine@network0.org

Let me preface this article by saying I love my privacy and I love well designed tools, but I find privacy more valuable. I've been using various tools online for all sorts of things such as Google Reader for news aggregation, Gmail for email and calendaring, Gtalk for IM, Evernote and Google Docs for notes and documents, Delicious for bookmarks, Flickr and Picasa for photos. As you can imagine, files, pictures, notes are everywhere and it's not easy or fun to back up - that is, if backing up your content is even possible! Another concern of mine was to have a backup plan in case one of the services I depend on decides to go belly up. Where would I be then? Could I get *my* data out? Who is going to have access to my data? What if they turn into Facebook and constantly change their stance on privacy? I couldn't sleep or stop thinking about it. This led me to build my own solution using open source tools that you can get on the net.

Now, I'm not a programmer, but I've figured out a good bit on PHP and MySQL based applications and I'm pretty comfortable using them, so that was a part of my requirements, since I wanted to install this on my web host. I'll also point out there that it would be a good idea to get a static IP and an SSL certificate so you can encrypt your applications if your host allows it.

Now, on to the applications!

News Aggregation: RSSLounge or Gregarius

Greader (Google Reader) is a great RSS aggregator and I love the features, but I wanted to have more control of my privacy without the advertisements, so I found RSSLounge. It is really stable and fast, and has an easy to manage subscription list. There is also integrated search and, not to

mention, built in tagging and organization which is a must have these days. You can check RSSLounge out at http://rsslounge.aditu.de/. Gregarius is also a good choice since it has all of the above mentioned features, but requires a bit more database maintenance (when it has about 10,000 articles, it starts to get slow). Gregarius does also offer theming support and has a plugin architecture so you can customize it yourself. Gregarius can be found at http://sourceforge.net/projects/gregarius/.

Email: Crystal Mail or Roundcube

GMail has arguably the best webmail interface out there. My host comes with IMAP support and I decided to start using it. Most webhosts use Squirrel Mail (http://squirrelmail.org/screenshots.php) and, while it is functional, is pretty ugly. I found that Crystal Mail or Roundcube is a wonderful alternative. They both have built in calendars and address books and are very active projects. I would recommend either of them for webmail needs as it just comes down to a matter of taste. You can find Crystal Mail here at http://www.crystalmail.net/ or Roundcube at http://roundcube.net/.

Chat: Jabber

GTalk is still good for IM and I still use it, but since my host also provides a free Jabber service, I decided to use that, so keep this mind if you're shopping for a web host.

Notes and Documents: Wordpress

It may seem that using an entire content management system for notes and documents is overkill, but I believe that having a really flexible and active project to maintain my most important notes and documents is really important. The flexibility of themes and plugins make this one of my favorite tools. It is even possible to make Wordpress be your image gallery. I have found that there are two key plugins that I use on my particular installation: Inline Editor (http://www.wpxpand.com/plugins/inline-editor/) and Postie (http://wordpress.org/extend/plugins/postie/). The Inline-Editor plugin is exactly what it sounds like. I can edit my notes directly on the Wordpress blog without having to go to the admin panel and Postie allows for more fine grain control of email posting. This makes it easier to post notes and documents since I can fire up Thunderbird and shoot off a quick email or even use my phone. I would also like to point out that that it is imperative to keep Wordpress up to date so it is secure in order to prevent any unauthorized access. You can get Wordpress at http://wordpress.org/. It is also worth noting that many webhosts can install Wordpress for you if you like.

Bookmark Management: SemanticScuttle or Insipid

I had been using Delicious for years, so I had quite the collection of bookmarks and I didn't want to lose them. Luckily, I found that there are a few projects that will fit the Delicious toolset perfectly. SemenaticScuttle (http://sourceforge.net/projects/semanticscuttle/) is an open source project that aims to essentially build your own Delicious type service. This was a bit too much for my needs, but it is still an attractive option. I opted for Insipid (https://neuro-tech.net/insipid/), which is really lightweight and even has Firefox plugins, so you can easily add bookmarks. It is worth noting that both of these tools support tagging importing Delicous bookmarks, so migration to these is a breeze.

Evading Content Filtering: PHProxy

Every now and then, you may come across a website that you can't view at work or at some other location (2600.com - *ha!*). This wasn't originally in my needs, but it comes in handy, so I figured I'd throw it in. I also am not responsible for any trouble you get yourself into by using a tool to evade content filtering. By installing PHProxy (http://phpr0xi.sourceforge.net/), you get a mini URL bar and can browse freely by having your web host proxy your browsing to you. It is worth noting that there are a million different ways to do this, but that's for another article and this works well enough in a pinch.

Webserver File Management: PHPfm

PHPfm (http://phpfm.sourceforge.net/) is a great web-based file manager that has come in handy countless times. I consider this an important part of the toolbox. It is invaluable for when you are at a location that does not allow FTP or SFTP access or you need to do nearly anything else file level related.

Security

As for security, I keep all my apps in a separate directory off my main website (i.e., somesite.com/apps) and that is further protected by an .htaccess file password authentication and requires an SSL connection as to prevent snooping while using my tools. If you are shopping for a web host, I would recommend keeping that in mind or seeing if your current web host can provide this level of service. It is entirely possible to run this off of your own server as well; the beauty of all of this software is that it can all run on nearly any platform.

I hope you found this interesting and useful. Just remember: "It's not paranoia if it's real."

Shoutout to Jimmy Grizzle for helping me appreciate my own privacy.

Add a User With Root Privileges Non-Interactively

by Pipefish
pipefish@anonymousspeech.com

My intent for this article is to provide several neat methods that can be used when working with *nix systems. I wanted to share this with folks because I think these are very useful. I'll not only tell you how to create a user whose privileges mirror root's, but I'll tell you how to do it in a non-interactive environment (via two methods). To perform these, you already need root/sudo privileges on the system in question. Of course, you must own the system or have permission to muck about with it! Doing illegal things is bad for Karma... probably.

Why?

Why would you want to add a root user if you're already root? There are probably many cases for this, but one I constantly find myself in is during penetration tests. I find myself with a non-interactive root shell on a Linux/UNIX system after taking advantage of some exploit. If I want to be able to install packages to the system (maybe a SOCKS proxy or nmap?), or do anything with much depth, I prefer an interactive environment, one where I can actually see what I'm doing and get the full benefit of TTY; namely stdin, stdout, and stderr. Some companies won't let you change root's password (or don't like it). Also, some distros don't allow the root account to log in via SSH/telnet (without changing conf files). So how do I get into the system via ssh or telnet if I can't change root's password? Add a user with the same UID/GID as root, of course! Sounds easy enough, but it's tough in a non-interactive environment where any script or program that requires user input doesn't work as expected. Below we'll bypass those limitations.

Let's Do It!

The first method to add a user non-interactively is very simple. Add a user to your own system with a password and the group membership you want, then copy and echo the lines for that user from your passwd and shadow file into /etc/passwd and /etc/shadow on the target system. I'll show you how to add a user that shares a group/userid with root in the next section, but a quick note on how: you'll want to add a user to your system with the same privileges/memberships as root.

Example: When I created a user called "test" on my system with a password of "password", this is what that user's line looked like in my passwd/shadow files:

```
my /etc/passwd:
test:x:0:0::/home/test:/bin/sh
my /etc/shadow:
test:$6$aae8qp/j$r0c.
HGGbDsIRRLc4
➥x2htq588feJ3rsjzFvZOd/nawNkpA.D
➥.kLzzAZA4UhfMc7zU8B13WuFu8oC8eK
➥rXxaYxa/:14929:0:99999:7:::
```

On the system you have non-interactive access on, simply do this:

```
echo 'test:x:0:0::/home/test:
➥ /bin/sh' >> /etc/passwd
echo'test:$6$aae8qp/j$r0c.
HGGbDsI
➥RRLc4x2htq588feJ3rsjzFvZOd/nawN
➥kpA.D.kLzzAZA4UhfMc7zU8B13WuFu8
➥oC8eKrXxaYxa/:14929:0:99999:7::
➥:'>> /etc/shadow
```

The second method is a bit more involved, but can also be used/modified to script adding/changing users' passwords non-interactively. This method also demonstrates using the python crypt lib and is a good way to learn some *nix administration.

For systems that support the useradd (not adduser) command, do the following:

```
useradd username -o -u 0 -g 0
```

The -o switch allows multiple users to have the same uid/guid (0 is root). The user will have no password at the moment. In normal operation you'd simply issue the passwd command, but this will not work with a non-interactive shell. Assuming you have access to a system with python installed (and since the system you're

logging in from is backtrack 4 R1, I know it's got python!), simply enter python and hit return.

Now you're at the >>> prompt. Type in `import crypt; print` and hit enter. Next, type `crypt.crypt(<password>,<salt>)`, where password is the password you want to assign to your user and salt is the salt value you'll use in encryption.

The output you'll receive will be the encrypted password. Copy it down.

Now type `usermod -p encrypted password username` and hit enter. This assigns your new user a password. Now you can ssh in and have full interactive root access to the system, and root's password is unchanged.

For systems that support the pw command (FreeBSD for example), the steps are similar but the commands are a tad different. I fooled around a bit and found a working set of commands.

```
pw useradd -o -u 0 -g 0 -n username
```

The above adds the user with no password. The steps are the same for generating the encrypted password, so use python and crypt from above and copy the output.

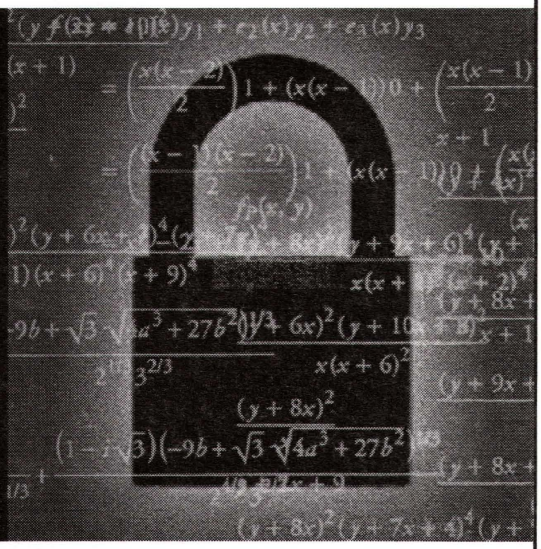
Then enter `echo encrypted_password | pw usermod -n usename -h 0`

The above command assigns the password to the user. Now, just as before, you have an account with root privileges, but the system's root account is unchanged.

You may ask yourself, "Why would I choose the second method rather than the first, simple echo method?" In most cases, you'll find the first method will work just fine. But the second method may be helpful if you're experimenting with scripting user add/modify actions or in some strange instance when you don't have the ability to echo commands into the passwd/shadow files.

I hope you find this useful. Good luck and happy hacking!

Simple RSA Encryption or Human-Calculable Encryption



by b3ard

At first glance, learning cryptography can be as tedious and time consuming as many other things in life, just as learning a new language can be difficult in getting familiar with the strange syntax. There are different kinds of cryptographic methods, one of them being the RSA public key cryptosystem. For a quick overview for those of you who aren't familiar with RSA, the RSA cryptosystem encrypts and decrypts messages/data by the use of public and private key pairs.

Public and private key pairs work like this: Bob and Sue have their own private and public keys. Bob and Sue both generate their own unique key pairs (using a program like the open source GnuPG), which each contain a public key and a private key. Bob doesn't know Sue's private key and vice versa; they only share their public keys. Bob uses Sue's public key to encrypt a message. Sue's public key can be received in any number of ways, such as an online repository, in an email to Bob, or copy-pasted from Sue's website. Even a hardcopy printout of Sue's public key would suffice in a pinch. Sue receives Bob's encrypted message, and uses her private key to decrypt the message encrypted by her public key.

In practice, public and private keys are generated by using large prime numbers, and by large I mean prime numbers that are over a hundred digits long. But for quick and fast encryption when all you have is a pen, paper, and maybe a calculator, you will use extremely small prime numbers or "weak" keys to generate your cipher. For those of you who are wondering why on earth would we want to do something like this, it is because it really only works with the notion that those around us have no formal experience with cryptography, which means that there will virtually be no general or special purpose methods of attack against our cipher. So where might this be effective? The work environment where Big

Brother is always watching, prison as a get-out-of-jail-free card with the inmates by teaching them how they might communicate openly should you ever find yourself there, who knows. Where I am at currently, all electronic communication is constantly monitored, but not post-its with numbers on them.

In getting started, the only tool that you may want is just a calculator that supports the modulus or "mod" function. Windows has a sufficiently advanced calculator and so do most Linux distros, otherwise get ready for some mind-working, elementary long division, and multiplication. All the mod function does is take the remainder of two numbers when divided into each other. An example for clarity would be 7 mod 5. 5 goes into 7 one time with a remainder of 2 and thus, 7 mod 5 = 2. I will refer to the "modulus" result as the actual number that will be used in both keys and "mod" as the function when performing mathematical calculations.

With that, we will now choose two small prime numbers. Continuing with our example numbers of 5 and 7, let p=5 and q=7. Two other numbers we need are our modulus (also called N) and r. We multiply both p and q to receive our modulus. (p)(q) = modulus = N. So, N=35 and that will be our modulus for both our private and public key. Note that the message chunks must not exceed the size of the modulus itself. For r, let r = (p-1)(q-1). So, r = 24. From here, we need to find two more numbers, e (encryption exponent) and d (decryption exponent), such that their product mod r is equal to 1, or in equation form: ((e)(d) mod r) = 1. The method we will use to generate e and d is: (r+1), ((r+1)+r), (((r+1)+r)+r), etc. What we are essentially doing here is reverse-engineering numbers whose modulus e and modulus d will be 1. This gives us a list of candidates to then factor out, thereby obtaining e and d. The list of candidates from r = 24 is: 25, 49, 73, 97, 121, 145. The list goes on but 145 will do. We'll let k = 145. We now factor out k to obtain e and d, which is 5 and 29. Let e = 29 and d = 5. To double check this, we plug e and d back into the previous equation ((e)(d) mod r) = 1, which ((29)(5) mod 24 does equal 1, so we're good. The reason we did not pick any of the previous candidates is that we never want a number that, when factored, gives us a result of the same number. An example would be 49, which results in 7 and 7. This would leave us with the same public and private key, which isn't a good idea. Also, picking a prime number is no good, for obvious reasons (clue: you can't factor primes). We now have our public and private keys: e = 29, d = 5, also expressed as (e, N) and (d,N). Private Key = (29, 35), Public Key = (5, 35).

The next step involves actual encryption, since we have our algorithm and the variables we need to generate the message. Because it is impossible to multiply A by 5 (not counting hexadecimal), we need a substitution method for our letters in order to turn them into numbers. It can be as simple as A=1, B=2, C=3, and so on, but nonetheless this is important because the recipient of your encrypted message will need to know how to turn the decrypted numbers back into readable text.

The message we are going to encrypt will be just one word, "problem." After substituting each letter for its number according to the simple substitution method mentioned above, we get: p=16, r=18, o=15, b=02, l=12, e=05, m=13 (16, 18, 15, 02, 12, 05, 13). Now we will use the RSA algorithm to encrypt and decrypt each number, using our public and private keys that we just made. Remember, in practice you would use your counterpart's public key, not your own. And he or she would use their own private key to decrypt the cipher. To encrypt: `Cipher = (Message)^e ➥mod N`. So we take the first number, 16, and raise it to the 5th power which is 1048576. Then we apply mod N to this result, which gives us 11: 1048576 mod 35 = 11. By doing the same operation for all six remaining numbers our Cipher = 11 23 15 32 17 10 13. And that's it - this is the encrypted message. To decrypt: `Message = (Cipher)^d mod N`. Decrypting with our private key transforms our ciphered message back into its original form, which then can be substituted into its readable format. (11)^29 mod 35 = 16, 16=p.

Ideally, for this kind of fast and quick encryption method, announcing or publishing your public key in some wide open area is not recommended. At least not in the way conventional public keys are implemented or intended to be used. Instead, including them in your cipher is much more effective for our purpose. This eliminates others (who might know a thing or two about ciphers) from easily cracking your cipher through factoring out your modulus, which would be extremely easy given such small numbers. A way to do this is by including your public key at the end or beginning of each cipher, or just your first one to make it known to the recipient(s). Many other ways exist, but this is just one method to get the ball rolling.

In summary, remember to ensure that your p and q are prime and that your k factors out to two different numbers. Break your message into chunks so that the message length is shorter than your modulus. Also, remember ((e)(d) mod r) must equal 1, otherwise the cipher will not work.

A special thanks to l0j1k for giving me the idea and encouraging me to write this article.

Booze, Nosiness, and City Terminals

by th3linguist
th3linguist@googlemail.com

0x00: Mother Tongue

English is not my mother tongue. So if you stumble across strange formulations, have a laugh or figure out which language is my mother tongue. If you are right, maybe I will send you a prize.

0x01: Preamble

Do you know this situation: You walk through a park or a city in the midday sun, with swollen eyes from last night's boozing. Birds are singing, head is ringing, and passing cars are honking - and you swear to yourself: Never again will booze touch my throat! Never! Ever! Again! OK, so far, so familiar, and a few weeks ago that was th3linguist's status - and because of that he had a collision with a city terminal.

So, let me explain what a city terminal is. I live in a district town in the south of Germany (hint!). We have a palace there and a nice pedestrian area with a lot of shop windows and flower tubs. In 2005 the city council decided to do something for the tourists and assigned an IT company to install four information terminals in the city. The first generation consisted of a desktop PC, built into a control box with three displays on top of it for ads and another display with a keyboard for user control. As a tourist (or a being with fingers), you can enter search terms ("Where is the next cinema?" "Where is a drugstore?" ...), send photo e-cards, and even print out a city map. Nice idea! But in 2005, I wasn't really interested in exploring the technique behind it. I had to deal with a disappointing love affair and with a job and and and... (crazy time).

0x02: Nosiness

In 2009 the IT company was assigned to modernize the terminals. They constructed four new city terminals with one big touch screen (we seem to be the i-generation). There is still a cam to take photos and send them via email, the printer function is not any more, and the UI is now shiny and very, very colorful. On that hangover day, I walked the pedestrian area with a headache. Suddenly I stood in front of one of these terminals and said "Hello! Could you please step aside!" It didn't. So I touched the screen and played a little bit with it. Nothing special. No Internet browser, no porn, no access to the mayor's mail account. But now I was nosy. I wanted to know how these terminals worked and I thought it would be great to show some nasty pics on the display. As you can imagine, there isn't a button called "Publish own content" or something. So I started thinking....

0x03: Getting in Touch

How to get remote access to the terminals? Well, I took a photo, sent it to a garbage mail service, and rushed home. In front of my computer I downloaded the e-mail, opened it with a text editor, and read the email header. Et voila, there was the sender's IP address.

I started Vidalia, configured my browser properly, and surfed to the IP. What would happen? I saw the same UI as on the city terminals.

A first conclusion: Mail server and web server are using the same address. Furthermore, the city terminals are not standalone, they are just clients. I needed more information. I started gathering it using "whois" and reading the website of the IT company. On their site they stated that they were using their own content management system called mcOne4all. Not much information about that on the net, but they were offering a test account on a server. To get a test login, I would have to give them a valid mail address and telephone number. No way!

0x04: Going Deeper

So I surfed back to the terminal's web server. The URL looked something like this: bk.interXXXXXcity.de/de/5. I did a right-click on an image and selected "show image". The URL of that looked like: bk.interXXXXXcity.de/images/user1.gif. Bang! From the ID (../de/5) to the real path. I started the beloved bash and gave a torified wget a chance:

```
torify wget -r http://bk.interXXX
➥XX.de/de/5
```

I had to wait about 45 minutes, but then I had a mirror of the website. I created an empty file and did a

```
cat foo*.html >> empty_file.txt
```

All right, there was one file with all the good content. Again, I used the linux onboard tools:

```
cat empty_file.txt | grep http://
➥bk >> links.txt
```

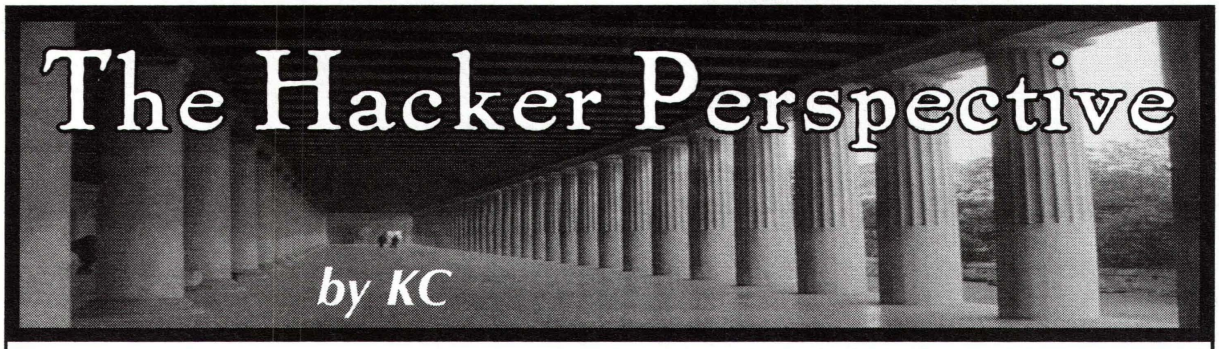
The file links.txt should now contain all accessible, absolute links on the webserver. After a little bit of handicraft (grep, grep, and more crap), I found a link to "http://bk.interXXXXXcity.de/mcCMS". Well, obviously. That site redirected me to a login form. Not so interesting at the moment. I focused on another link: ../mcCMS/editor. There was no way I could start the editor directly via an *.html or *.php. But... directory listing was enabled!

0x05: Climax

OK, to cut a long story short: In the directory ../editor/popups, I found a complete listing of the parts that are composing the admin interface - without access control. Lovely!

0x06: Cleanup

Why I wrote this article? I think it is an example of the old fashioned way of hacking. Be nosy, be creative, be - well - nasty!



The Hacker Perspective

by KC

A hacker is someone with a need to know. A hacker is not merely a person with a strong technical aptitude, adept at math or technology or mechanical work, for those are all the means that we use to satisfy the need. The need is that of curiosity, a desire to peek behind the curtain and take a poke at what makes the world work.

The world is an iceberg, hiding the great majority of itself behind interfaces. The front-end experience, I have discovered, is magnitudes less interesting than the underlying infrastructure. Behind every door, every panel, in every wire and circuit, there are gears and cogs, bits and bytes. They move and spin and flash entirely without pretension, an enormity in an instant.

We are all interconnected, part of one machine. Set aside the metaphysical for a second and consider the physical implications of this. Often less chaos than ordered discord, my actions have real and lasting consequences, and that is exciting! Sometimes the results are small, sometimes they're large, but for every action, there is a reaction.

"Why" drives me onward, encouraging me to discover why something is. "Where," "what," and "how" are greater together as "why" than they are alone. Larger than the sum of its parts, "why" is an insatiable curiosity as great as any hunger or thirst I will ever feel. Is there a limit? In the end, the limit is where I draw the line.

The question that keeps me hacking is "what happens if?" "What happens if I pull this gear out?" "What happens if I type this?" "What happens if [anything]?" Far beyond computers, electronics, or hardware, hacking is an application of perpetual discovery. A hacker is never bored, because there will be an infinite number of questions to be asked, long after the time for questions is finished. In my own mind, I find endless possibilities, and all it takes is a hack or two.

The question shouldn't be "why hack?" but rather "why not?" How can someone possibly go through living experiencing it in the most shallow manner possible, never looking past what's presented? It's unfathomable that someone could spend a lifetime with a toe in the shallow end, for fear of the unknown. In the deep end there be monsters, but they're far outnumbered by the wonderful experiences that come with discovery.

A life on the surface is possible because apathy is addictive. It's easier to take things at face value and accept them, because that path is already trodden. Someone has asked all the questions that need asking and provided the answers, and this is abhorrent. I don't want to just push the feeder bar and receive my pellet: I want to know why a pellet comes out, and what happens if I push it as fast as I can.

Hackers are made, not born. Every one of us was born with the potential to be curious. It doesn't take a genius to be a hacker. If this were the case, hackers would be few and far between. The difference, as with most facets of a person's personality, lies in the upbringing.

My father was a carpenter, plumber, and all-around handyman. He never sat me down and said "now you're going to learn to like tinkering, or else." Instead, I watched him solve problems on his own, often making the product better in the process. Many children believe their father can do anything. When said father comes pretty close on a domestic scale, that leaves a lasting impression. Very early on, I learned that with a little bit of knowledge and the willingness to try, a person can accomplish anything.

I started out taking apart old appliances and toys. If a screwdriver didn't work, I took a hammer to whatever had piqued my curiosity. It was an inauspicious and often messy start, as my mother could attest. True too, it resulted in a few smashed items that weren't meant for my own brand of exploration, but it was a fantastic way to start learning about the world around me. To this day, nothing makes me happier than disassembling something to see how it works. It was a childhood and set of experiences that I wouldn't trade for anything.

Raising a hacker doesn't have to be so dramatic. If there's one thing a parent can do to encourage a child to dream big, it's to simply encourage them. Show them there's more to the world than meets the eye. Learn a little bit about nature and then share it. In fact, learn about anything and share it with anyone, for that is the other side of hacking.

Hacking is inherently social. This is contrary to stereotypes, but stereotypes are inaccurate misrepresentations of the noblest of pursuits. A hacker does not tinker and poke and prod for himself. He does it to say to others, "Look what I did!" There is no small measure of hubris in a hacker, but the best hackers temper this with a desire to share and collaborate.

Hacking is the noblest of pursuits because it is a desire to make something better and share it with the world, and this holds no small measure of dignity. It is a meta-pursuit, encompassing all jobs,

hobbies, and walks of life. Everything around you can and will be hacked to improve it. If this were not true, we'd still be in the Stone Age, content to let technology flounder.

Hacking saved my life. On top of the usual growing pains that come with adolescence, I fought off depression and suicidal urges all through my teenage years. I could have easily turned to drugs or petty crime to express my outrage at the imagined inequalities of the world. Instead, I turned my self-righteous fury into determination. Suddenly, every puzzle was a challenge. With a tenacity that served me well later in life, I attacked each challenge until I mastered it.

I now know that a great many people go through adolescences similar to my own. Unlike many, in hacking I found an advantage and an outlet that most teenagers don't have. If it wasn't for that outlet, I would have imploded years ago.

When the self-centered despair of youth became overwhelming, I retreated into the quiet of my mind. I shut off the outside world and lost myself in pursuit of knowledge. The logic and order of a well-engineered system always helped me to become centered. I spent most of a shift at my first job attempting to fix a three-hole punch with a drywall screw and a power drill, during one particularly trying day. What really irks me is that I know if I had had another half an hour, I could have done it.

The hours I spent tracing the workings of various machines became a kind of meditation, with "why" being the mantra that continues to set me free. Every hacker meditates in a similar fashion. Every time you lose yourself in a project for hours on end, you're meditating. There's nothing New Age or mystical about it. All that happens is the outside world gets shut out, allowing your brain to focus squarely on the task at hand. People pay a great deal of money to learn how to do this, and for many hackers it is inherent.

In the end, what I gained was an appreciation for what matters, and a few skills that have served me well. Perhaps not surprisingly, I found myself employed in the IT field right out of university. What was unexpected was the level of success I found almost immediately, because I was used to solving problems and coming up with solutions.

I have created a future for myself that is brighter than I would have dared to dream, all because I let my imagination run wild, and never stopped to wonder if I was stranger for it. Engage, envision, and above all else enjoy what you're doing, or you're no further ahead.

The skills a good hacker has are skills that all in-demand employees possess. Troubleshooting, ability to work independently, and attention to detail are skills that pay the bills, no matter the industry you find yourself in.

To future and current hackers alike, I urge you above all else to find balance in your life. Learn to appreciate the time you have to tinker and experiment. With age comes responsibility, and those responsibilities will take precedence. Though I'd love to be ears-deep in new toys, the last thing I hacked was my kitchen sink. Unglamorous, perhaps. Messy, certainly. But I fixed it by myself, using the same skills I would have used to hack anything else. Logic, reason, and intuition are the greatest tools at my disposal.

Never stop exploring. Read everything you can get your hands on, actively engage in the world around you, and never stop asking "why." The "why" will often echo for lack of takers, but ask it anyway. Shout it, if you have to.

We are the face of change, the propagators of progress. If you want a Buck Rogers style future with hovercars and jet packs and robotic maids, then go out and create it! There are no set limits; the only limit is how far your vision goes.

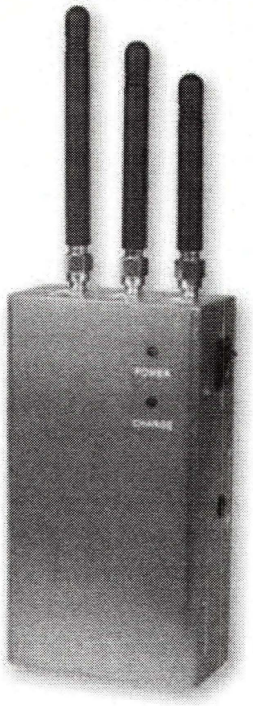
One day, we will all of us be gone, but the changes we make to the world will live on. Bring up the next generation of hackers to the best of your ability, and never forget the sense of wonder that got you started down this road. I will forever be grateful to have had a family that let me take apart things with a hammer and let me make my own mistakes. Someday, I will do the same for my own family.

Keep your horizons broad and your eyes open, and your life will be richer for it. We are far outnumbered by people happy to follow in the footsteps of giants, hopping from shoeprint to shoeprint. Blaze your own trail and enjoy the trail while it lasts, because nothing is forever. Hack on.

KC is an IT consultant by day. He spends his time outside of work pursuing purely analog hobbies, having recently graduated from smashing things to building them.

Hacker Perspective is a column about the true meaning of hacking in the words of our readers. We're interested in stories, opinions, and ideas. We're now accepting submissions for a limited time after being deluged the first time we did this. The column should be a minimum of 2000 words and answer such questions as: What is a hacker? How did you become one? What experiences and adventures did you live through? What message can you give to other aspiring hackers? These are just suggestions - you must choose your own points. If we print your piece, we'll pay you $500.

articles@2600.com or 2600 articles, pob 99, middle island, ny 11953 usa



How to Protect Your Car from Radio Jammers

by Beyond

This past September, an interesting bypass of car locks was believed to have occurred in Surrey, England. Police in Surrey theorized that a gang of car thieves were, and possibly still are, utilizing radio jammers to help gain entry into vehicles. According to a local resident, who perhaps was nearly a victim, he was unable to lock his car with his remote in the presence of an individual dressed in unseasonably warm clothes. When this individual was no longer around, the car and remote cooperated as if nothing out of the ordinary had ever happened. Police believed that the individual was dressed in unseasonably warm clothes to conceal a radio jammer. When an intended target tried to lock his/her car, the jammer, already turned on, would prevent communication between the remote and the car and thus prevent the car from being locked remotely. The car owner would unknowingly walk off leaving the car unlocked, allowing the thieves uninhibited entry. Ingenious, to say the least. Theoretically there's nothing preventing this from happening, but realistically? I'd like to see a bit more proof than just one testimonial before I'm convinced. Nevertheless, it's possible, and you, I, and everyone else could be a victim. Let's look at this vulnerability a bit more in depth and discuss a few ways that we can all better protect ourselves and our property.

First, let's do an experiment. You're going to need a car remote and Internet access. Look on the back of the car remote and find a number listed to the right of the FCC ID. Now, point your browser to the FCC's ID Search database which is found at: `http://www.fcc.gov/oet/ea/➥fccid/`. This database contains public information related to a searchable FCC ID. Next, we're going to input the FCC ID into the form found on the previously linked page. In my example, I'm going to use my Ford Ranger remote. Its FCC ID is CWTWB1U345. Don't worry; it's not unique or linked to my VIN. I share it with hundreds of thousands of other people. When I hit submit, I get some basic information about my device such as its manufacturer, Alps Electric Co., Ltd., and their address. I also can get some reference material, such as photos of the device's internals or test reports, by clicking "Detail" under "Display Exhibits." That's all well and neat, but what we're looking for is our device's operating frequency. You can find that by looking at the last two columns from our initial search return: Lower Frequency in MHz and Upper Frequency in MHz. In our case, along with just about every vehicle on the road, its 315 MHz. Toyota, Lexus, Mercedes, Chevrolet, etc. all use remotes manufactured by separate companies, such as Alps, that utilize the same 315 MHz as required by the FCC in the United States. Now, I'm sure you're thinking, "But Surrey is in England, well beyond the jurisdiction of the FCC!" Right, but when your biggest customer, the United States, requires a certain frequency on one of your products, you're going to conform to that request and your entire product line is going to reflect it. Simple business strategy, but I digress.

A quick search on Alibaba.com produced a jammer capable of operating on the 315 MHz frequency at a range of between 50 and 100 meters for roughly $35 USD. I'm sure a more intensive search could produce a cheaper and perhaps more reliable device, but you get the point: what they need to prevent you from locking your car via a remote is easily accessible and not very expensive. It's also not exactly rocket science to operate, either, which probably explains why they're in this line of work, if you want to call it that.

So how do you protect yourself, your friends, and family from this? Exercise common sense. If you don't hear your door locks "move" into the locked position after pressing the corresponding button on the remote, try again. Still nothing? Then manually lock your doors. A jammer isn't going to prevent you from manually locking each door or pressing an "All Lock" button in your car. It's not going to unlock them either once you leave. If your car remote doesn't work, don't panic and don't become paranoid. There's usually a common explanation to the above scenario: a low battery. Your car is already locked at this point; even if someone is trying to jam your remote in the area, you've already thwarted their attempts. Take your remote to the local auto parts store when you get a chance and have them check your battery's strength. Breathe a sigh of relief when they tell you it's dead and you didn't just almost become the latest victim of a radio jamming gang.

Air Intercepted Messaging: A Revisit of POCSAG and Radio Privacy Issues

by Malf0rm3dx & Megalos

A couple of times every year, I find myself wading through the boxes of electronic components, parts, wires, and miscellaneous odds and ends that I've accumulated over the years. Usually this is done in an effort to make space for new gadgetry or by the demands of my wife who threatens me with bodily harm should I not get rid of some the electronic "giblets" that threaten to take over the house. I guess this is common tradecraft for those of us with the hacker gene and love for technology.

A recent purging seemed like all the rest, but, while rummaging through the old electronics cables and connectors, something caught my eye. From its facade it looked like just a regular RS-232 connector. Upon closer inspection, I realized that I had stumbled across my old L0pht Heavy Industries data slicer. Oh the memories! My mind quickly ventured back to the old days when pagers were the prevailing technology for communications. I remembered all the fun and adventure that was to be had with a simple radio frequency scanner and a data slicer. As I thought about all the information that could be obtained when using these types of devices, it occurred to me how significantly society has changed from a privacy perspective. I remember these devices being able to intercept and decode sensitive and extremely personal medical information, personal messages to loved ones, alerts and warning messages from devices that were being monitored, even detailed data captured from airplanes as they flew overhead. As I pondered all of the things that were possible with these devices in the late 90s and early 2000s, I wondered, could it still be possible to collect all of the same sensitive information today? Were pager systems still a viable technology and something currently used by corporations and institutions? Did they broadcast personally identifiable and private information to the world in an unencrypted manner? My curiosity had to know the answers to these questions and I found myself dusting off my old radio scanner and collecting up the necessary cables to find out.

A Word About the Technology

For those of us who grew up in the years when personal pagers were considered a new consumer technology and were all the rage, the acronym POCSAG is not an unfamiliar term. POCSAG (also known as Post Office Code Standardization Advisory Group) was born from British telecommunications and was the forefather of numerous other paging protocols including Super POCSAG, Flex, Mobi, and several other proprietary ones. POCSAG is a fairly simple Asynchronous Protocol using a Frequency Modulation (FM) known as Frequency Shift Keying (FSK) for transmitting data. Data is transmitted in 32-bit blocks using a frequency shift of +/- 4.5 kHz on the carrier frequency. The frequency shift represents a 0 or a 1 depending on the shift up or down. Originally, this enabled data to be sent at 512 bits per second. 512 bits per second is slow by any standard, but viable when sending plain text. Subsequent versions and predecessors of POCSAG provided significantly more bandwidth. Most notably among these is the FLEX protocol. FLEX is a proprietary protocol developed by Motorola and is still used on many pager systems today. Similarly to POCSAG, FLEX uses Frequency Shift Keying (FSK) to transmit data. The FLEX pager protocol is able to achieve much higher speeds including 1600, 3200, and 6400 bits per second by using a four level modulation of the carrier frequency.

The transmit frequencies used for pager services spans the gamut of the VHF and UHF frequency bands. Pager services started in the 35 MHz range and go all the way on through the 900 MHz space. Now that pagers are not as widely used by consumers and are more utilized in certain industries and special use groups, the frequencies seem to be weighted in a couple of areas. 152 MHz to 158 MHz is a hotspot for many medical and hospital paging systems. 420 MHz through 540 MHz is a collage of corporate, industrial, and privately owned paging systems. And 920 MHz to 940 MHz seems to be the prevailing frequency for the remainder of consumer pagers. There is no doubt that someone who takes the time to carefully scan through all of the VHF and UHF frequencies would find additional spots where POCSAG or its predecessors are being transmitted.

A common trait amongst all of the pager protocols is their inherent lack of security. As with many communication protocols, those used for paging systems were not designed with security in mind; a topic that has been detailed before within the pages of *2600.* POCSAG and FLEX broadcast data completely unencrypted and often over a significantly large geographical area. While this may be fine for simple communications of non-sensitive information, it is completely unacceptable for personally identifiable information such as names, Social Security numbers, date of births, addresses, or the specifics of medical treatments being given

to a person. The telecommunication companies rely on the fact that transmitted pager data is obfuscated using FSK modulation as a means of security. They also hide behind laws such as Counterfeit Access Device Law, 18 USC 1029, that that make it illegal to use a radio scanner to knowingly or with intent, eavesdrop on a wire or electronic communication. And let's not forget the Electronic Communications Privacy Act, 18 USC 2510, that prohibits anyone from intercepting messages sent to display pagers both numeric and or alphanumeric. And, while these laws are in place, there is absolutely no technological means that is stopping a person from accidentally or intentionally intercepting these transmissions and using them for personal gain. Knowing that this threat exists, it would be deplorable for companies or any organization to send sensitive information across these systems, yet that is exactly what is happening!

The System Setup

Because such tasks would be illegal as defined above, I'll state what a person "could do" and the type of information they "could see," should they be so inclined to intercept POCSAG and FLEX transmissions with a radio scanner and a data slicer. This information is intended to be for educational purposes only and to provide awareness to the issues. The equipment needed for intercepting, collecting, and decoding pager transmissions involves three key components. These are: a radio frequency scanner, hardware or software data slicer, and a software package for interpreting and storing messages.

Radio Frequency Scanner - A programmable radio is the key component to intercepting pager transmissions. The device can be any programmable radio that has the capability of monitoring the frequencies that are used for pager transmissions. Radio scanners, also known as police scanners, make an excellent choice as they cover most frequencies used by pager systems and often come with line-level out or signal discriminators that make accessing the raw signal stream transmission significantly easier. With that said, any radio with an earphone or line-out jack that covers the appropriate frequencies can be used in a pinch with a little dedication and patience.

Data Slicer - Data slicers act as the decoder and interpreter of pager transmissions and come in a dizzying array of capabilities and functions. The purpose of the data slicer is to take the received radio transmission, interpret the FSK modulation, and convert it to 0s and 1s so it can be converted back to plain text. Data slicers can be obtained in either hardware or software based formats. Hardware data slicers can be purchased or built for very low cost. Hardware data slicers typically come in one of two formats, either two level or four level modulation decoding. The difference between them will allow you to decode different protocols and at different speeds. A software data slicer can also be used. Software data slicers work in much the same way as hardware data slicers. Software data slicers utilize the line-in jack of a sound card to collect and decode the radio transmissions. While software data slicers have the same capabilities as hardware ones, they are often harder to configure and more prone to error and distortion than their hardware brethren. The majority of pager transmissions that are alphanumeric are typically transmitted at 9600 baud. A hardware four level data slicer is required to consistently decode transmissions at these speeds. Many free software data slicers exist including "Paging Decoder for Windows (PDW)," available at `http://www.gsm-➥antennes.nl/PDW/pdw.php?lang=eng` and "Multimon" for Linux, formerly available at `http://nathan.chantrell.net/old-➥stuff/radio/radio-scanning/➥pocsag-pager-decoding`. (Searching for "Multimon Linux" will uncover other sites.) Both applications allow you to use a hardware data slicer or a sound card as input devices.

Decoding Software - The decoding software receives the decoded radio transmission and converts it back into text. The primary difference between the decoding software applications is the number and complexity of paging protocols that they support. The two applications mentioned above are both excellent for decoding POCSAG and FLEX transmissions as well as numerous others protocols. Both the applications are capable of decoding and interpreting pager transmissions. There are numerous other good decoding software applications that only work with the hardware data slicers including "WinFlex" and "Pocflex" available at `http://homepages.ihug.co.nz➥/~Sbarnes/pocsag`. "Paging Decoder for Windows (PDW)" is by far the most current and supported pager transmission decoding application available and it's free!

The Test

As an example setup for this experiment, a Uniden BC898T programmable scanner was used along with a two level data slicer designed by L0pht Heavy Industries in the early 90s. These were used with Paging Decoder for Windows (PDW) version 3.1. The scanner has a 1/8" line-out jack on the front side as does the RS-232 connected data slicer. Application setup is extremely simple. Simply select the hardware interface and the type of pager protocol to decode. By default, the PDW 3.1 will default to using a hardware data slicer on com1 and will decode POCSAG and FLEX at the highest speed supported by the data slicer.

Pager transmissions have a very distinctive sound and are easily found by scanning up and down the various frequency ranges. For this experiment, the focus was on low speed alphanumeric transmissions in the VHF range. Low speed

transmissions are easier to consistently collect for obvious reasons, even with low signal to noise ratios. Medical and hospital pager systems fall into the VHF bands and appear to be concentrated in the 152MHz to 158MHz space. The 150MHz band is very close to the two meter amateur radio band and is supported on a very large range of radios and scanners alike.

A word about tuning and configuration if using software and a sound card as the data slicer: Software data slicers are very temperamental and require some trial and error to get the right combination and consistent results. Start by opening the squelch completely so the signal (and noise) are received by the application. Volume should be set high or full on the radio and on the input for the sound card. This gives the application a loud and (hopefully) clear signal to interpret. Most software applications used for decoding transmissions have a signal meter of some sort. Use it! You are going to need at least 60-80 percent to get discernible and usable data.

All right, enough already with the "what" and "why." Let's get to the money shot! So what type of data can be collected? With the above defined equipment and configuration, collecting entire transmissions is pretty easy. Most of the software decoding applications parse the data in a fairly clean and straightforward manner.

Address: Channel Access Protocol (CAP) code. Used to uniquely identify each receiving device.

Time/Date: Yup, you guessed it - time and date of the received transmission.

Mode: Protocol version used in the transmission (POCSAG, FLEX, etc.)

Transmission Type: Alphanumeric, numeric, or tone only.

Bitrate: Baud rate of the transmission.

Data: This is where the actual number or message is contained. Message lengths can vary depending on the receiver and the service provided.

In the below examples, I have blurred out the sections of the material to protect the privacy of the individuals, IP addresses, and company names. Even so, it is clear that a person can extrapolate all sorts of personal and sensitive information from the intercepted transmissions.

In the first two examples, we see the type and details of medical information transmitted by hospitals about their patients. The first details an unfortunate lady going through chemotherapy and having a hard time with it. Not only are we given her name, date of birth, and ailment, but enough detail that a crafty social engineer could wreak all sorts of havoc at the hospital or with her personal life.

```
0646297 21:48:46 07-12-10 POCSAG-3  ALPHA  1200  1373
0630428 21:48:47 07-12-10 POCSAG-3  ALPHA  1200  1373

0617158 21:48:48 07-12-10 POCSAG-3  ALPHA  1200  DEBRA [redacted] 73F DOB 082337 7027770 HAD CHEMO YESTERDAY HAVING BURNINGUNDER LEFT BREAST ------- 12/07/2010
08:38p KN ------- called home paged him and faxed it tohis office
```

In the next example we see the personal details of a young woman who suffered heart problems.

```
0646254 21:56:44 07-12-10 POCSAG-3  ALPHA  1200  CLEAN:[redacted], JENNIFER F29 MN:7216627 RM:H85701 CS:Clean
DR:100214 [redacted] JUAN C DI:HEART FAILURE/SEIZURE, ETIOLOGY UNKNOWN, TOD: 9:23PM
```

In another example, we see an alert message containing an internal IP address, domain name, and email address information for an Oracle server that apparently is running out of space.

```
0665204 21:49:38 07-12-10 POCSAG-3  ALPHA  1200  FR:OracleManagementServer <IS_DBA_SUPPORT@[redacted]>>EM Alert:
Critical:ICP_lvhingenxlvpg.[redacted] 172.18.76.143/91% of archive area G:\oracle\flash_recovery_area\ICP\archive\ is
used.:Dec 7, 2010 9:48:31 PM EST
```

In these last examples, we see a collage of personally identifiable information (PII) and company information that could be used for identity theft, credit fraud, or as the basis of a social engineering or system compromise attack.

```
0663404 22:00:04 07-12-10 POCSAG-3  ALPHA  1200  FR:<HRS@[redacted] org>>HRS:TOMORROW [redacted], DEBBIE DOB:7/19/73
SN:15880[redacted] *NO INSURANCE* /ABDOMEN AND PELVIC PAIN / BELIEVES TO BE DUE TO FALLING

0663220 00:00:56 08-12-10 POCSAG-3  ALPHA  1200  FR:XT@[redacted] COM>>CONFIRMED-583250 [redacted], Luz 03/25/1955 FROM EMERGENCY ROOM GIVEN IV&O2
Returning Home 54 Hamilton St. [redacted] family has been notified.

0915943 00:12:24 08-12-10 POCSAG-3  ALPHA  1200  FR:@[redacted] org>#7NK/CAD MSG: *[redacted] ALSTRAUM 3121 STATE HILL RD @COLUMBIA
COTTAGEROOM 38 0043 82 YOF /FELL OUT OF BED /BLEEDING FROM FACE /ALSO APPEARS TO BE HALLUC Sent by:Information Exchange to [redacted] EMS
All CALL through Ber
```

The above examples are just a taste of the type of data that is constantly being broadcast across the airwaves with no encryption or security of any kind. While the messages are encoded by the senders for brevity purposes, it's very easy for anyone to decipher the data and fields in the messages. It should be mentioned that a person can very easily discover the frequencies being used by their local stores, companies, and hospitals. These details can be found by Googling information discovered in the captured pager transmissions or by searching a particular organization's site, or, if you are really adventurous, by looking on the back of any of the pagers that you are interested in capturing data from.

Despite the fact that pagers have gone out of vogue as a mainstream communication tool, it's very clear that niche industries are still using them very heavily. And since the technology is not as widely used, it's not getting the attention that it should.

In Conclusion

I've learned several things while doing this research. First off, just because a technology is old or has been replaced by new tools and solutions doesn't mean that it isn't still viable or being used. More importantly, if the technology is of significant age, its compliance to best practices and security are probably sorely lacking. Like most readers of *2600*, I take privacy very seriously and I try to do all the right things to protect my identity and my credit. To think that my preventive measures can be thwarted by some jackasses sending my personal information over the airwaves for all to receive is very disturbing to me. This brings up the question of liability. Is a company or hospital liable for sending PII data over the air in an unencrypted manner? Are the telecommunications companies liable for not meeting minimal security practices on a protocol that is decades old? Regardless of the answers, the bottom line is that telecommunications cannot hide behind laws as their justification or safeguard against transmission interception. As long as telecommunications are being sent in an unencrypted manner, people will intercept them and use the information for nefarious purposes.

Auditing the MiFi2200

by pnorton

The Internet has become much more than a series of tubes to many of its users, providing near-instant access to a variety of information as well as remote access to services. The technology has extended beyond the conventional wired realm into wireless communication as well.

While access is ubiquitous to some, one runs into circumstances, hopefully temporary, where one is unable to connect successfully to an access point.

All too often, one's efforts to connect are frustrated by access control or encryption technologies. Circumventing WEP or MAC filtering will be left as an exercise to the reader. WPA is acknowledged to have a respectable level of strength, by contrast, when implemented successfully. The novice hacking enthusiast will be grateful for a little help.

What are the weak points of the WPA implementation process? While perhaps technically and cryptographically sound, the weak link in the chain is the human implementing the security. The framers of WPA (and its successor WPA2) were relying on the implementor of the communication system not to write the password down and store it in a vulnerable location, to physically secure the access point, as well as to choose a cryptographically significant password. It is this last article which is perhaps the most vulnerable to attack.

A friend of mine who works in the infosec industry once speculated that something like 95 percent of humans, when choosing even an important password, will choose from a hypothetical list of perhaps one million passwords. This plays right into one of the weaker points of the WPA family of encryption process, which is the handshake. In the case of one system that I audited, human error made things even worse. For this reason, the reader's attention should be drawn to one popular access point, the MiFi2200 Mobile Hotspot, a portable 802.11b/g AP consid-

ered novel because it is a first generation IP over 3G. The 3G communication protocol will be familiar to most of our readers as the protocol that allows cellular telephone access to the Internet.

That's why I like the MiFi2200, because the geniuses at Virgin Media have made it possible for me to have roaming Internet access pretty much anywhere that I can get a phone signal. Cheap. Pay As You Go. I love Sir Richard Branson.

So if I could fault the good people at V. Media for anything, it's that one of the default security settings on the MiFi2200 is somewhat bad. The default setting for the WPA key does not take advantage of the full consortium-defined keyspace available to security implementors. It's an uncomplicated eleven-digit number. That means that there are less than one hundred trillion possible combinations. Does that seem like too many to try?

Perhaps we can narrow it down further. On the original unit that I purchased, the default encryption key was an eleven digit number and the ESSID was a slight variant of "VirginMobile MiFi2200." I got a little curious and poked around a bit, discovering that the password was the same as the decimal representation of the ESN.

Of course, this made me even more curious and so I had a look at another two units, discovering the same coincidence. Could it be that OEM set all of the 2200 series encryption keys to the ESN? Only testing will tell, or confirmation from the vendor, heh.

Before you begin auditing anything, keep in mind that you need to have a solid background in counter forensics if you want to get away with anything. Learn the law and how to avoid getting ensnared in it. Also, you'll need to create yourself a dictionary file with all of the conceivable numbers that might be used as default passwords. The manufacturer's code will be the first eight bits of the ESN or the first three digits, which is 091 for my device. This leaves only 18 bits for the manufacturer to assign up to 262,144 codes in this batch, hence the vulnerability. Software like pyrit will tear through a small set of PMK, and even the aircrack-ng suite should be able to accommodate this sort of attack.

I would like to outline the testing procedure in general terms:

- Find all Windows installations in your laboratory, and format the hard drives. Install Linux. Maybe back up your older data, maybe not. Consider starting life fresh.
- Install Linux on your attack laptop. Install the aircrack-ng suite, either using your distribution package manager or compile from source to increase your credibility. Ubuntu is good. Gentoo is better. If you have trouble with these, you might want to use a LiveCD such as Pentoo, or Backtrack if you are a noob.
- Go someplace where a lot of people, particularly businessmen or traveling salespeople work. Perform a scan for VirginMobile named 802.11 wireless networks. The iwlist command from the iwtools suite works well in combination with a modified grep command if you are working in a target-rich environment.
- Having obtained the ESSID of your target, next you will need to intercept the WPA handshake. As such, you may find it helpful to dissociate any connected clients using the aireplay-ng tool in the aircrack-ng suite. This tool is remarkably effective. As the client disassociates, it will likely reassociate with the access point during which time you may intercept the handshake. The handshake is the weak point of the crypto process. *Protip:* Use two network cards so that you can send DEAUTH packets with one while listening in promiscuous mode with the second one for handshakes.
- With the handshake successfully intercepted, use the aircrack-ng forcing or the pyrit forcing utility to find a collision. For this, you will need to specify your dictionary file (q.v.).

Please note: I researched, discovered, and publicized this hack because I have abundant respect for the MIFI equipment marketed by the Broadband2Go service by Virgin Media. Although I won't admit to making a clandestine audit of their resources, at the least I feel comfortable saying that I was impressed by their security setup, and will continue to proudly be a Virgin customer, publicizing only a minor bug. Along these lines, security enthusiasts should recognize that minor to moderate security bugs in technology products and services are no more egregious an error than when you order (patriot) fries from McDonalds and they don't have enough salt on them. In essence, security bugs should be accepted as a fact of life, and any security professional who gets publicly bent out of shape about them is likely insincere and is in most cases either a blowhard, a profiteer, or a gloryhound. If you're successful, you may have temporarily granted yourself free anonymous Internet access.

Also note: I've worked professionally as an authorized pen tester for the past five years, a job coveted by many of the younger security professionals that I meet. However, I'd like to be the first to disclose that among the many jobs I've held in my life, being a pen tester is among the lamest jobs that I'm familiar with. If I were a bartender, at least I'd be getting paid in alcohol.

Shout outs to: D0, alexbobp, Kevin Mitnick, Stephen Watt.

No shout to: anyone with cissp, ceh, or other lame certs that only prove that you lack skills.

Voice of the People

Reaching Out

Dear *2600:*

I've been a fan of your publication for quite some time before subscriptions became available for Kindle, at which point I finally got myself a subscription. Part of what I love about *2600* is the sheer gravity of some of the great hacks, especially the ones that were serious risks to education systems and big businesses. What I don't understand, though, is how it seems that the talk of hackers being misrepresented in the mainstream media (a redundant issue at best) has overshadowed the fact that hackers should be seeking more allies, rather than distancing ourselves. It seems very easy to simply write off anonymous script kiddies and their DDoS tactics, but it also seems far too easy to lose the reasoning for these attacks in the arguments against the attacks themselves.

Just because they're not real hackers doesn't mean that they don't have anything to say on subjects that are clearly near and dear to the hacker community, especially in the realm of Internet censorship. It's easy to talk about how the world is becoming less free and how it's relevant to hacking. But it seems absurd to chastise people for using the only tactics they know when talking, writing letters to senators, and publicizing the truth clearly accomplishes nothing. And for those of us who condemn their tactics as crude - while admitting that going about things the legal way is completely ineffective - is it not a show of our own complacency to fail to present alternative options?

Hackers are depicted as villains in the media largely because of these kinds of blunt, poorly thought out attacks by non-hackers, but is it any better that we can only seem to depict ourselves as victims of this same media? Setting information free can be a heroic act, but at some point we may come to realize that information gives people a reason to fix things, not the ability to do so. At some point, we must realize that in a world where every aspect of the governments/businesses that run things - without our consent - is stored in a vast network of computers, every aspect of our own finance is controlled and stored in a vast network of computers, and (nearly) every aspect of our own social interaction is stored in a vast network of computers, (computer) hackers are the only people left with the power to enact any real change. The very existence of this power in an unjust society can only serve as a reminder of our responsibility to use it.

Basically, what I'm trying to say is that as hackers, we need to stop whining and come to a very simple realization. We are freaking Spiderman, and it's now our job to go out and save the world whether we like it or not. And it probably wouldn't hurt if we recruited more Spidermen in the process, perhaps even from the swarm of script kiddies. What do you guys think?

And, as a side note, I thought I'd mention: Never bother composing an email on a Kindle. It's a serious pain in the ass.

D351

You raise good points in recognizing the potential value of anyone who understands what the issues are, along with the difficulty of emailing on Kindles. We certainly don't want to dismiss anyone prematurely. However, to say that "talking, writing letters to senators, and publicizing the truth clearly accomplishes nothing" is doing precisely that to others, whether they be the "enemy" or the unenlightened masses. These methods should never be written off as pointless, no matter how frustrating the process may become. The very nature of hacking tells us to keep trying against the odds. Why should this be any different? Plus, we find that we win many allies by rationally presenting the facts, not by simply shutting down the opposition, which is all that DDoS attacks accomplish, apart from gaining sympathy for those we oppose. If we truly believe in what we're saying, then we fight on that. Only when we start to have doubts in ourselves should we resort to desperate acts that accomplish nothing.

New Stuff

Dear *2600:*

Before I delve into the main point of my letter, I'd like to say two things. The first thing is that I've long admired the articles and letters printed in *2600* and find them to be both informative and interesting to those of hacker mindset. Secondly, I'd like to preface by expressing my hope that this letter does not come off as a shameless advertisement or self serving, and I'd simply like to expose readers to a possible site of interest. The site in question is 1337-chan.org, an image-board with a posting style very similar to other popular forums like 4chan, 7chan, etc. I decided to write because I was inspired by both my own desire to see the site prosper and gain a dedicated community, but also to give hackers (and other tech-minded individuals) a simple and accessible way to discuss their practice. I found this second reason especially important after reading a recent *2600* letter where a reader asked for such an outlet. Sharing of ideas is key to hackers who yearn for knowledge and I feel that being able to share information in real time within the framework can be a very useful tool. To wrap up, thank you very much for reading (and hopefully publishing) this

letter, and thank you for any and all future support.

(Side note: The "1337" in 1337-chan is not used to infer we're "31337 h4X0rs," but only to meet the "number_chan" theme. In reality, we just love the topic and would enjoy sharing knowledge in the community.)

Shadow
Admin at 1337-chan.org

And now, the community will judge you. We wish you luck.

Dear *2600*:

Long time reader and fan here. I'm working to promote the OWASP AppSec USA 2011 conference, where we'll be celebrating our tenth year as an organization. Would it be possible to get the following listed in the Hacker Happenings page of the next issue of *2600*?

OWASP AppSec USA 2011
Minneapolis Convention Center
Minneapolis, MN
www.appsecusa.org

OWASP is a nonprofit and keeps the price as low as possible for conferences (e.g., AppSec USA 2011 is $335.75-$385.75 for non-students at the moment), but one thing of note is that students get in for $75 with student ID and proof of enrollment, and so I was hoping that would fit the criteria of not being ridiculously expensive. Everyone's welcome, especially students and people who support open contribution.

Adam

It's a bit pricey for the general public to qualify for the Hacker Happenings page but it's an event worthy of note so we'll help you spread the word here. It takes place September 22-23, incidentally.

Meetings

Dear *2600*:

I'm looking for a person who can hack into an email account. I was thinking about attending the meeting in Philadelphia at 30th Street Station, and asking around at the meeting for someone who could help me. I just wanted to make sure that the meeting still takes place. Are there any other details I need to know about finding the meeting place? Do you think that I will be successful in finding someone while there who can help me? Thank you for your anticipated help.

Sherlock Holmes

The meeting still takes place at these coordinates but you're not likely to be successful in your quest as stated. Why? Because this is almost precisely how the mass media and lawmakers view hackers - as individuals who spend their time breaking into other people's email accounts, changing grades in school, transferring money to their bank accounts, stealing identities, launching missiles, releasing chemical agents into the atmosphere, and not paying for music. We're rather sick of it. In fact, asking such a question at a gathering of hackers just might be the final straw and, since we're so dangerous, there's no telling what we might do when enraged. But here's an idea. Why not go to the meeting and ask for advice on how you can protect an email account from the sort of person who would want to break into it? You'll find that people will offer very good advice on how to safeguard your privacy and, if you're clever, you might be able to use that knowledge to figure out where the weaknesses are. What you do beyond that point is on you.

Dear *2600*:

I am a PhD student in the public administration program at the Maxwell School of Syracuse University and would like to attend an upcoming Friday meeting. I would like to interview several *2600* people. These interviews will be used for research purposes only.

My dissertation examines how knowledge practices in contemporary social movements affect administrative practices. The open and free software movement is one of my (three) social movement cases. Based on my research, people working for government organizations benefit from the knowledge that the free and open source movement developed. It appears to me that many movement people informally collaborate with their peers who are employed by government agencies or some people employed by government agencies also participate informally in movement groups. In my case, I look at the *2600* hacker community as well as the community of civic technologists ("civic hackers") in New York City.

I would like to interview those people who (1) would like to share their opinion/stories on informal knowledge exchanges between the *2600* community and government agencies (excluding law-enforcement agencies). (2) I am interested in learning the opinion of *2600* people about civic technologists who (in my theory) represent the same free and open software movement and its hacker ethics. Civic technologists are involved in government-oriented projects, such as developing open 311 systems.

I believe you have had many PhDs who examined hacker culture in the past. However, my main argument that it is good for government officials to learn from people is something that might be fun for many of you to discuss (or trash).

Is there anyone who would want to introduce me to the *2600* crowd? I don't want to wander around like a complete stranger (which I am, of course).

Vadym

This letter came in a while back so you've hopefully already talked to some people. This is a fairly standard request that is received now and then for our meetings all over the world. We welcome the opportunity to be able to show our perspective to people who are interested in looking at it from an angle that perhaps we haven't thought of ourselves. For those interested in talking to hackers at the meetings, you needn't worry about not knowing anyone or standing out in any way. We meet in public because we want to meet the public. You'll find some remarkably enlightened individuals who at-

tend and, while there is no one voice that speaks for the entire community, if you converse with as many as are willing to talk, you should come away with a sense of what we're all about. And we'll probably learn some interesting things from you as well.

Dear *2600:*

I would like to attend a meeting in L.A. Do I need to pay, give notice, or just show up?

Jesse

Just show up at the appointed time on the first Friday. All of our meetings are free and open to anyone who wants to attend.

Dear *2600:*

Hey, I live in the Netherlands. Do you have meetings there too?

Peter

In fact, we do. There is a meeting in Utrecht. If that's not convenient, feel free to visit our meetings page at www.2600.com/meetings to see how to set up or find a meeting in your area.

Dear *2600:*

I am moving to an area that doesn't have any *2600* meetings except if you want to drive 100 miles to the nearest one. I was wondering if there are any other procedures or are they all on the meetings website?

Paul

The website pretty much says it all but we do prefer that meetings not be too close together, since the idea is to meet people you don't already know from your local area. A hundred miles is a hike but some might be able to swing that once a month and, if it's possible, it's well worth the trouble. Meetings work best in cities since more people are around and they're easier to get to.

Dear *2600:*

I've been a reader for a while, but have never attended a meeting. I see the Virginia Beach meeting is still listed in the meetings area. Do you happen to know if this is still going on? Or maybe have the contact info of whoever heads it up? I'm interested in going.

Icarus

If it's listed, then it still exists, at least until enough people say it doesn't. We don't give out any contact info but many meetings have official websites and you might be able to make some connections there. Otherwise, just show up and bring a friend if you can. It's not unusual for attendance to vary from month to month and, if you find it's not as big as you expected, you can play an important role in improving that by spreading the word and getting the enthusiasm level up. This is why every meeting belongs to every attendee equally. We all have the power to make it worthwhile.

Dear *2600:*

I didn't see any listing at all for West Virginia, so I was wanting to make one for Clarksburg. I haven't ever been to any *2600* meetings, but I would love to go. All are very far away! I would like to see one for Meadowbrook Mall.

Also, you can tell everyone that this place (www.almostheavendesserts.com) has a computer you can use for free and they don't monitor it very much. As far as I can tell, there are no restrictions. I have to type fast because I don't want them to know that I wrote this.

Anyway, I was wanting to see if you can post a wanted meeting for West Virginia or something. If not, then I understand. Plus, I won't be checking on this account since I have made it here. LOL

jason

And another great meeting enters the gestation period.

Clarifications

Dear *2600:*

Just an FYI. Lived in GTMO for six years and the payphones from Naval Base GTMO (27:4) are actually not "pay phones." All local calls in the base are free and all long distance calls from these phones have to be made with a calling card.

DR

From the pictures, they do appear to be pay-phone-like in nature and these days it's not at all unusual for such phones to no longer take coins. Other than that, we'd like to know of any specific operational differences along with more detailed pictures.

Dear *2600:*

In the article "Bash Bash Bash!" by Douglas Berdeaux (27:4), there are several instances where pairs of apostrophes (') have been replaced in the printing by smart quotes. This makes the shell scripts difficult for a person to read, and impossible for a computer to execute.

The first one is at the bottom of page 6, where the sed command should read: sed -e 's/ /\/g' -e 's/\-/\\-g'

There are numerous others involving the quoting of arguments to sed. Three more at the top of column 2 of page 7, in the l33t translator. Another one three quarters down that column. Three more smart quote replacements of apostrophes in the script at the bottom of column 1 of page 8.

Adding to the confusion is the author's use of back-tick substitution at the bottom of page 6. The line could be rewritten using $() instead, as: MEDIA$(echo $1 | sed -e 's/ /\/g' -e 's/\-/\\-g') This is much more readable.

carl

Thanks for the input. We hope you appreciate the humor of your last two sentences to anyone who isn't a programmer.

Dear *2600:*

Many thanks for an interesting magazine.

I do have a couple of minor corrections/alternatives for the "Bash Bash Bash!" article in 27.4.

Douglas Berdeaux has an example on how to use a shell script to make VLC not spawn a new window every time he clicks on a video file in Nautilus. And though it probably works, it's an example of bad practice. A way better method would be to always run VLC with the "--one-instance" flag and

never issue killall.

It's also a bad practice issue with systematically using the -9 flag for killall, as SIGKILL is the dirty method to end a program. As such, it should only be used as a last resort when getting rid of unwanted processes. So, in case you still want to end the process and launch anew, -15 (SIGTERM) is a better first choice. (It's also the signal that will be used by kill and killall if no signal has been specified.)

zarck

Dear *2600:*

In 2009 and 2019 under the handle p4tn0s and aesun, I wrote several articles for *2600*. If at all possible, I wouldn't mind having my real name associated with them.

j

And yet you only give us one letter of it. It's OK, though. Time travelers can't be expected to remember everything.

Dear *2600:*

I love reading your magazine. It's always full of interesting articles.

In the latest feature (28:1), there was an insightful article from Oakcool on why he (or she?) likes ebooks. And, for the most part, I agree with the article, except for one of the last advantages that was mentioned. He mentions that the cost is usually lower. I wish that were the case. I've seen happen on Amazon's website that the Kindle version actually costs more than a hardcover version. Technical books often do this, but I have seen novels that do this too.

And on the cost issue is where Oakcool's argument breaks down a little. A paperback or a hardcover edition holds a resale value for me as a consumer. I can buy a paper book, and the price matters a little less because I have the option to resell it later and get a little return on my investment. Probably won't make a profit, but it does lower the total cost of the book for me.

With ebooks, I don't have that option. An ebook, especially one with DRM, doesn't have any resale value. And that, coming from a consumer's standpoint, means that ebooks should come down in price a lot more. In other words, even if an ebook would have the same price or even a slightly lower one compared to a paperback or a hardcover, the ebook itself holds more costs for me compared to a dead tree book.

Please note, I do not mean that the ebooks become worthless in value. They can still hold the same emotional value as a paper book. I just can't resell it and recoup on my investment if I want to.

MadJo

Electronic Publishing

Dear *2600:*

Having only just caught up on my reading, I noticed you're now selling the Volumes as PDFs in the store. This makes me extremely happy, and I will definitely be purchasing these collections if you continue to sell them. Any chance we can get the entire back catalog in PDF as well?

The Atomic Ass

This is possible if there is demand for them. We believe the contents are terrific and ageless for the most part, but each of these projects takes a good deal of time and effort to assemble properly. We want this to be done right and the support we've gotten so far is very encouraging.

Dear *2600:*

I noticed in the last edition and on the website that you are now digital. I downloaded the latest edition to my wife's Kindle and was impressed. I also noticed it was available for Nooks. My question is, since it is DRM-free, can us life-timers possibly get a PDF, or I would happily pay an additional fee to get a lifetime subscription of PDFs sent to my email. I travel a lot with the Army so it might be a month before I get my zine after it is waiting for me.

Just a thought.... Now if we could only convince *QST* to go digital.

Michael

For now, the paper and electronic versions are separate entities. We don't have the means to do a lifetime subscription through the Kindle or Nook and, because of our deal with them, we can't offer PDF versions at a lower price, which a lifetime subscription would inevitably wind up being. All of this may change in the future. Just consider that little more than six months ago, we had nothing at all in an electronic version - and now the field is rapidly expanding. The future is going to be pretty cool.

Dear *2600:*

I just wanted to say a few things about what you are doing. First, I am *so* happy that you started to have *2600* offered for the Kindle. Your great work didn't go unnoticed - in fact, just the opposite! I have always had a desire to understand how and why things worked like they do. I thought a "hacker" was a bad thing. After reading my first ever *2600* that I stumbled upon in the Kindle store (unaware of your existence), I realized I was a hacker at heart (only a few "hacks"). I realized that it was not a bad thing to be a creative person who could think outside of the box, thus making it better for the people who were stuck plugged into the box. Hackers do things to understand, make things better, different, or interesting with a non-malicious intent.

Would the world be a better place if everyone could think outside of the box? Why is it that "hackers" are mostly associated with electronics? There was a social hack by someone in the issue that I read and it made me start thinking. I'm in an honor society and I have heard lectures by famous people who were successful basically because of social "hacks." They didn't accept the normal answers and they wanted more. They kept on trying from several different approaches until they had the result they wanted (in some cases bending rules/laws)! Is this not a hack? They are some of the most successful people because of how they thought outside of

the box. Your magazine has changed my perspective and opened my eyes to even more possibilities. Awesome work!

Thinkican

Welcome aboard. Thinking outside the box is indeed more or less the theme of the hacker world, and, as you note, in the lives of many people who become successful at what they do.

Dear *2600*:

I just set up a monthly subscription for the Kindle edition of *2600*. I wanted to write to you guys to let you know how excited I am to finally have your zine in electronic form. I ride my motorcycle to work every day and the real estate in my backpack is pretty small, so being able to store all of the issues on my one small device is awesome. Although I did have a one year, or two year (can't remember), subscription a while back, once that ran out, I'd forget to go buy the newest one at Barnes and Noble or Borders or wherever, so I'd end up getting one maybe once a year. Now I don't have to worry about it - it just comes automatically. I really hope this new way of publishing your magazine works out and you are able to continue to create and publish this awesome zine.

Brett

We've had a few bumps in the road but we're getting to where we want to be. We only hope more publishers give the new technology a chance, as right now there are relatively few who are approaching this openly. What we've found is that there is tremendous support for electronic publishing. One of the things holding it back is the misguided notion that readers of ebooks and ezines won't pay a reasonable amount for their favorite publications. Not only will they, but, as we hear every day, there are people all around the world being reached in this method who are much harder to find in the traditional paper approach. We will always be a paper magazine because that is something truly special. But there's no reason we can't keep trying to be more. How else does the future happen?

Dear *2600*:

I was wondering if you guys had plans to release the Winter 2010-11 issue on a format other than for the Kindle. I only have the Kindle app for iOS and it is not listed as a supported device on Amazon's website.

Jeremy

By the time you read this, Volume 27 (all of the 2010 issues recompiled as an ebook) will be available DRM-free in a bunch of formats. If this does as well as the previous volume (which we released at the end of 2010), we will try and get our previous issues compiled in a similar fashion. You should also have no trouble grabbing the current issue individually.

Dear *2600*:

I just wanted to let you know that I read your article about the changing landscapes of information and content, and shortly thereafter purchased a digital subscription via my Amazon Kindle. While I have friends at work who purchase the mag in paper format (and I'll occasionally purchase a hard copy when I see it), I respect your hacker spirit to choose to publish in open digital formats. I believe in what you are doing and I hope it will be a success. I also want to let you know that I love the format that you have configured for the Kindle edition. It is really easy to navigate and laid out really well.

Thank you for all of your efforts over the years standing up for free thinking, creativity, artful expression, curiosity, and passion.

William

Curiosity

Dear *2600*:

As a Canadian, I am used to paying higher prices for almost everything in comparison to our southern neighbors. Books and magazines are no exception, and are generally priced 10 to 30 percent higher. The standard answer we used to get is that the price difference is due to the exchange rate. However, the recent U.S. economic downturn combined with soaring commodity prices has helped lift the value of the Canadian dollar above that of the U.S. dollar. As of this writing, one U.S. dollar is equal to 98 Canadian cents, yet we still continue to pay the higher premiums on books and magazines, including *2600*. The U.S. cover price for *2600* is $6.25 while the Canadian cover price is $7.15, which is almost a 15 percent difference (subscription price, however, remains the same). Clearly, the exchange rate currently has nothing to do with the price differences. I am curious if you can answer the question many Canadians have: what exactly is the reasoning behind the higher cover prices? I figured *2600* being considerably more transparent than big publishers would be able to provide all of us Canadians with an answer.

Sasa

We can't speak for other publishers, but we can tell you how it works for us. You are correct with your exchange rate data. The two currencies are close to equal most of the time. But what kills us, and forces us to charge more, are the delivery costs to ship issues from the States to stores in Canada. Even though the distance isn't greater than shipping to another part of our country, the rates sure are. (It gets worse overseas. By the time all of the charges are taken out, we pretty much don't get anything back.) While subscriptions and other orders to Canada cost the same as in the States, they really shouldn't due to the much higher postage costs. We may well have to adjust that in the future if it gets any worse.

Dear *2600*:

On your store, certain back issues are listed as "only available in full sets." So does this mean that you have to buy the other three collections for that volume to get it? For example, 1984-1987, I would have to buy 1984, 1985, 1986 to get the 1987?

Richard

No, we're sorry if this appears confusing. Those

four years are grouped together because they were always sold as full years, unlike the period from 1988 and beyond when we became quarterly and offered individual issues. What we're facing now is a depleting inventory which means we can no longer offer everything in the same manner. There are some issues we're out of completely and others that are very low so we're only offering the remaining stock to those people who buy entire sets. Eventually, those will be gone, too. As we expand our digitization efforts, we expect to preserve the entire collection in a way that's worthy of the material.

Observations

Dear *2600:*

I found this snippet in the "About the Author" section from Kevin Mitnick's new book *Ghost in the Wires:* "Kevin Mitnick, the world's most famous (former) computer hacker, has been the subject of countless news and magazine articles, the idol of thousands of would-be hackers, and a one-time "most wanted" criminal of cyberspace, on the run from the bewildered Feds."

I don't want to point fingers here. I am not sure who wrote this piece. I am, however, a little concerned about the line that says "(former) computer hacker." I would view this as Kevin distancing himself from the word hacker, and somewhat strengthening the misconceptions many share about the "hacker" culture/community. I can't say that I would do differently if I were in his shoes. I would like to think I would take on the label with pride, but after being demonized by the press, along with the perceived criminal connotation of the title... well, you understand.

I found the "would-be hackers" remark interesting, as well. I was just wondering what your thoughts were.

Thanks for all of your hard work on the magazine and the radio show!

drlecter

It is indeed unfortunate and not at all uncommon for the words "former hacker" to be used to describe hackers who have gone on to something else. We understand why a publisher might insist on this in order to dispel any image of criminals being rewarded with book deals. But it should be noted and resisted when they do.

Dear *2600:*

I don't know if you can help me, but you released an article by the LoU, so I thought you might know someone who can help. I'm not a hacker - in fact, I'm pretty busy raising my kid - but something has to be done.

In my home state of Arizona, our legislature, governor, and law enforcement have been overrun by neo-Nazi Mormon whack jobs who I am sure are up to no good. Our media has consistently backed off when getting to the dirt. So now our state has become the most backward - even behind Mississippi (no offense) - in the statistics and eyes of the world.

Some items and players: *NewTimes* newspaper started researching the Maricopa County Sheriff about his financial dealings and, after years of legal battles, the Sheriff ultimately arrested the publisher and suddenly the paper wasn't looking into the issue anymore.

Now the Sheriff's number two guy, Russell Pearce, is our State Senate President. He is the one who enacted SB1070 and is beholden to the LDS, private prison corporations, and is trying to turn anyone who cannot prove their citizenship in this state into a ghost. They won't be able to work, drive, rent, buy, etc.

And, of course, our governor is a puppet to these groups. All of this is available online.

Please help. They need to be hacked!

William

Where do we begin? Well, first off, back in 1999 we joined with various hacker organizations to condemn the idea of hackers being used to wage war against another nation (China, in this case), following some statements by member of the Legions of the Underground (LoU). Not exactly the same as releasing an article by them and sort of the exact opposite. But whatever.

We're aware of the problems in your state. The case of the newspaper owners being arrested back in 2007 was truly shocking and received a good degree of attention at the time. The newspaper has filed a lawsuit and you can still find many articles challenging the actions of Sheriff Joe Arpaio, who has been condemned globally for everything from human rights abuses to misuse of funds. Meanwhile, the overzealous pursuit and prosecution of those suspected of not having the proper papers is indeed cause for concern. It's not fair and doesn't do much for your case to blame this on Mormons, however, as these issues have been points of contention within that community as much as any other. The responsibility lies with all citizens, those who instill such policies along with those who don't do enough to stop them.

So now we arrive at your final point: that these folks all need to be hacked. Where do people get the idea that this is how problems are solved? Putting a clever slogan on one of their web pages and getting some attention is all fine and good, provided that existing content isn't destroyed in the process. We're certainly not opposed to people who know what they're doing digging in computer systems for evidence of corruption or for those already in the establishment to leak such information to the public. (Of course, there already is ample evidence that's been exposed, so we have to wonder how much more is needed to turn things around.) But we fear that what you mean (based on your initial reference to the LoU) is a denial of service attack, an action that has got nothing at all to do with hacking and simply is a method of silencing an opponent. This is the best way to gain sympathy for these people. Since their own words tend to come back to haunt them, is it really wise to shut them up? From your perspective, the more they say, the

better the chances of people seeing them for who they really are, rather than just making hackers into scapegoats yet again.

Dear *2600:*

Sometimes a *New York Times* web page will load but it will display an annoying pop-up. Often this pop-up seem to appear whenever there is extra information in the URL in the browser URL bar. From within the link, just select the question mark and everything to the right of the question mark, delete it, and then reload the link.

In the Chrome browser, at least, your page displays just fine. Every so often, with a new page, you will have to repeat the task.

I am not sure why the *New York Times* would put data into the URL after the question mark. Whatever the reason, your reading experience is greatly improved.

AnyPerson

Dear *2600:*

I'm not sure why you are having paranoid feelings about Verizon's lack of quality and customer service. Do you think it's any different for the rest of us? Seriously, they suck.

Dan

You're referring to the mysterious connectivity issues that we tend to get at critical moments that wind up lasting for days. We wouldn't call it paranoia so much as simply an observation of how incredibly unmotivated large companies can be when it comes to fixing problems of other non-large companies. What is particularly ironic in our case is that we have an SDSL connection through another company and want more than anything not to be a Verizon customer, yet Verizon keeps coming up as the reason for all of the malfunctions, cut wires, lack of maintenance, etc. Until there is true competition, this kind of thing can be expected to continue.

Dear *2600:*

Apologies if you guys have seen this, but on the web page for the proposed International Linear Collider (the particle accelerator that may replace the Large Hadron Collider at CERN) at www.linearcollider.org), the first picture you see is rather interesting.

Petar

Wow! At the very top of their page, in the first of a series of photos, is a picture worthy of our back cover that is simply a street sign for "Discovery Street" with a big "2600" on it. We don't think this is the address of either the International Linear Collider or the Large Hadron Collider. We also don't believe it has anything to do with that incident back in 2008 where some Greek hackers got into the LHC website and left a message that read "GST: Greek Security Team - We are Group 2600. Don't mess with us." It's all just a series of strange events that together comprise the nature of physics.

Dear *2600:*

Has anyone noticed that there are a lot of binary ironies in the years 2010 and 2011? You can tell you are a true hacker, or at least good with math, when you look at somebody's license plate expiration reading something like "10-11," and the first thing that comes to your mind is that it actually spells "02-03" in binary.

Jeff

Well, at least you're outside.

Dear *2600:*

This is too short for an article but from time to time I notice that people tend to bring the simple concept hack to the Letters to the Editor page. And so, this is.

I recently bought coffee at a McDonald's. Evidently the person at my register was a manager because an employee handed them a 50 dollar bill to authenticate. I noticed that the employee then went to the safe, which was right around the corner from the counter with an entry door which separated the front side of the registers from the back side where the employees are and the cooking takes place.

It was a chest-high safe, and it looked very heavy when the employee swung the door open. I had expected the employee to lean down and punch numbers, or enter a dial combination, but they didn't. The door just swung right open. That attracted my attention right away because it was out of the norm for a usual operation-of-safe pattern. They put the money in, and then swung it closed again, but I didn't hear it close.

This was on a Saturday, in one of the economically harder-pressed parts of town. Maybe the person who has the combination didn't show up to work and just phoned it in to someone, maybe they just do it so the manager can work the registers. Maybe the manager is permitting theft. Maybe they're waiting for their friend to come by and "rob" the store.

The point is that it's like McDonald's has gone and pre-hacked the safe for anyone to exploit. I don't doubt that it is likely an expedient method that an overtaxed, under-supported management must deal with: managers frequently must come up with stupid "fixes" in order to cross the line between higher-up constraints and lower-down demands and actual play of how the business works.

This is a clear anecdote, but moreover, it points to the "hackable" space in any business: a single point of failure precipitated by understaffing, or simply the plan not coping well with the reality of working the registers.

McDonalds, then, pre-hacks itself despite having a system in place. Just because they have a safe doesn't mean they know how to include it in the overall workflow, or that workflow doesn't have a kink that leads to the kind of situation I saw.

Nobody should break the law using this information: However, everyone should take a look at what the reality of their system is, and not just what the "plan" is, because they don't always match. Exploiting an open safe is not hackers' work. Hackers don't steal. Hackers delight, however, in pointing out the weakness of a system.

Note that I haven't, and am not, calling McDonald's. Can you imagine what a nightmare it would be to try to report an ill-used safe to the appropriate person in the corporation?

e-Z-e-kiel

We're not really sure that an unlocked safe in clear sight is anything more than McDonald's-style stupidity. It's an interesting observation and it might result in some corporate memos, a change in policy, or a few attempted robberies. But, as far as hacking goes, this isn't really on the radar any more than pointing out that some people leave their car doors unlocked, which could result in other people opening their doors. It's just not getting us excited.

Worries

Dear *2600*:

Umm, this is a bit of a concern. You say "If we decide to use it in a future issue, we will contact you at the address you've given us." Normally, magazines and journals will send an acceptance or rejection letter/email to any submission. I cannot simply sit on this hoping that someday you will respond.

If it is not your policy to make a decision and notify an author in a reasonable amount of time, then I will be forced to withdraw my submission and send it elsewhere.

Chuck

First off, we don't do things the same way as most magazines. Second, as stated in the part of the automated message to articles@2600.com that you didn't quote, we will let you know within two issues (usually much sooner) if we'll be able to run your submission. You only gave us two days before getting impatient. Finally, unlike lots of other publications, we don't assume ownership of your piece. You're welcome to resubmit it to other places, but we do ask that it be unpublished at the time of our printing.

Dear *2600*:

Since you don't even respond to submissions, I am going to have to withdraw my article and send it elsewhere. Thank you.

Chuck

It's probably for the best as you apparently expected a response to the previous letter within minutes. We don't think that even the slickest publication on Earth would have been able to move fast enough for you. We look forward to seeing who you settle on, although we're sure you've moved on to a book deal by now.

Experiences

Dear *2600*:

I'm currently deployed and, while reading your current issue, was reminded of an amusing incident involving one of your previous issues. I was on shore duty, and I worked with an organization tasked with conducting connected virtual online training with military assets around the Pacific Rim. Think MMOGs with horrible graphics. We were heavy into VoIP, networking, and tying together 18 different systems developed by 20 different manufacturers. Anyway, one day we were due for a site inspection by DISA (the Defense Information Systems Agency), yet another amusing acronym full of stuffed-shirts intent upon blasting our networks back a decade in terms of effectiveness. In preparation, I left a copy of *2600* on my desk. When the inspector came through the office to check that there were no passwords on post-its or thumb drives in the USB ports, he zeroed in on my magazine and stated in a huff, "Why are you reading *that* magazine?" I responded "Why *aren't* you?" Not expecting me to go on the offensive, our intrepid inspector vanished in a huff. I suspect he is still not a subscriber. Thought I'd share. Keep up the great work.

SanDogWeps

If only everyone in the military showed this kind of courage.

Dear *2600*:

Ready for this? After terminating my Ma Bell land line account, I went to my favorite grocery store and used my card for a discount. I don't carry the card with me as I have always used a telephone number to validate the account (from the earlier paperwork to receive said discount(s)). Was unable to use my old number. Found the card and it did not work either. Looks like Big Bro is watching closer than we care. Good ole NSA through Homeland Security.

orPHan

We seriously doubt there are people (or even a single person) waiting to disable your grocery store loyalty card the instant you disconnect the phone number associated with it. Unless they were actually calling your phone every time you used the card to verify it somehow, this strikes us as a not very interesting coincidence. Usually, such numbers are only used as a reference point and, if you know those ten digits, you must be the person attached to the account. All that said, we're certainly being watched now more than ever. But not because of stuff like this.

Dear *2600*:

I recently received an email query on a Craigslist ad that I had deleted a week prior. In the email, I was provided with a link to follow to prove that I'm real. It must have come from one of the email addresses that I'd responded to when the item was still available since it was to my actual email address rather than the obfuscated one that CL provides. The URL was as follows: http://wewantit.org/548749/go.php?lid=xxxxxxxxxxxx with the x's representing what appears to be a unique string of numbers and upper/lower case characters. Attempts to access the site without the unique string resulted in a variety of errors including what appears to be a homemade "server not found" page. I didn't want to use the actual string they'd sent me, as I suspect it would have flagged my email address as valid (in that I must be a valid sucker to click their link). I tried several variations of the string and was each time met with "Link ID not provided or invalid."

I may have to come up with a more expeditious means of creating and testing strings. It amuses me to no end that they've created a sort of authorized access validation system for their phishing website. I can see why they'd want to be careful though. There are all sorts of shady characters out there.

nrKist

This is indeed rather interesting. People who post ads get contacted from someone who appears to be interested in buying, but needs you to tell them a real email address via the provided links. These links only last for a short time and are designed to get you to reveal your actual email address, no doubt so you can receive all kinds of spam and nefarious content. It's unusual that you received such a request to your actual email address as that is what they're usually trying to get out of you.

Dear *2600:*

I'm writing because I have not received my winter issue of the magazine. I do believe this is happening because the Brazilian post decided to be extra stupid. Here's what happened: they decided not to deliver any parcel with an ID starting with LN (that would be LNxxxxxxxxxUS, where x is a number). Apparently, they reckon they are not getting paid enough to deliver those parcels. Now, that would be okay if they actually *told* everyone else that this shipping method was no longer accepted (first class mail from the United States, in this case). But no, they did not tell anyone, as it seems. They just decided to send every parcel back to the sender. And here is where it gets better: I went to the post office to ask about it, and even called the central distribution office in Rio, and they've told me that they could not be expected to enter the parcel's info into the system if they were not getting paid for that. Fair enough, except that they *do* enter the parcel's info into the system in order to send it back to the sender. Even better: this only happens when the parcel reaches the area's post office. Yes, the parcel goes to Rio, then they pass it along, knowing that the parcel will not be delivered, and it is passed along to another five post offices, every time to a smaller one, only to be returned when it reaches the final post office. And then it makes its way back through those offices and to the sender.

Seriously, they are wasting quite a bit of money just because they are too thick to send me a note asking me to pay whatever they believe would be fair. So, that's it. As far as I know, no one in Brazil has been able to receive any magazines from the U.S., nor any other parcel shipped by first class mail. That is very unfortunate for me, since I have renewed my *2600* subscription for another three years and have only been able to get the first edition.

What I've found out is that express mail still works, but it costs about three times as much. The other option is to put a stamp on the envelope, just as if it were a regular letter. This costs about one ninth of what first class does, takes just as long to reach its destination, and is actually delivered.

Ian

This story from Brazil is worthy of being in the movie of the same name.

Dear *2600:*

I've been a hacker for a while. I really don't know when you go from being a kid messing around on the computer to a hacker. Anyway, I was on a trip recently to Utah and the plane that I flew on had Wi-Fi. So I went onto my laptop and joined the Wi-Fi that was available. It turned out that I had to pay for it. I noticed that the URL started with https so, just to see what would happen, I typed in https://www.google.com and it worked! I could browse without paying.

I love the magazine and if you ever find yourself on a plane with Wi-Fi, try that trick out. (The plane used gogoinflight - I don't know if it works with every service.)

Dead Rabbit

Dear *2600:*

I find that my perspective is often shifted and sometimes the world I see is stood upon its head.

Several months ago, I received an email from an old girlfriend who I haven't spoken to in five years. We broke it off oddly and a wedge of silence had been driven between us for this time. So when I received this message, I attempted to chase the link out of curiosity, but it didn't work.

So I sent a message. I said, "So I received your message, but I couldn't open it. What's up?" She sent me a message back. Apparently, she had no idea that such a message was sent. But she started to make small talk with me again, which was nice.

Then I started getting a ton of these other messages and we figured out that it was some kind of email virus. So an email virus reunited me with an old friend and lover. Nice. What an awesome concept! Thanks to whoever wrote that one. I owe ya, buddy! I don't know why I didn't think of this a long time ago!

Jimmy

And so we discover the true nature of computer worms - to reach out and bring people back together. This could be a good defense for anyone who gets prosecuted for spreading one of these in the future.

Dear *2600:*

So, here is my story. I just turned 70, have taken a partial retirement, and am still looking to do some computer consulting work. My last career was with the federal government, including some of the three letter acronyms.

I guess I am a hacker at heart, as my first hack was when I was about 11 years old when a friend and I strung some wire between our houses and connected two phone handsets, powered by old railroad lantern batteries we collected along the railroad tracks (that had been thrown away when they were just about worn out). We failed. In the Marine

Corps, I was introduced to Morse code, wireless, and crypto.

A later play was in the 80s and the first PCs when I wrote and stored a simple program that mimicked rain drops falling down from the top of the screen that I would load and run on demo PCs in budding computer stores.

I was amazed to see what I did in the Fed, countless web apps with Java/Ruby that were "more secure" than client server or terminal services, or Ada code (which I am learning now). There is so much junk out there!

I hope to resume attending the San Francisco first Friday meetings again.

Coyote

We hope you do too, as you have a lot to share. We believe people at the meeting will appreciate this.

Dear *2600*:

I have been reading your mag for going on a year. In that time, I have moved from medium to max, and finally supermax custody. I am literally on death row. The BTK serial killer along with one of the Carr brothers are my neighbors. For about eight months, I have been in solitary confinement. When I was in a different prison (Lansing, Kansas), someone got into certain parts of their system through a law library computer on the LexisNexis network. For about three or four days, it was really like the Gestapo were going to get us.

And... here I am. I am out the door in six months. They moved me from one cell to another for the last four months after my phone in my cell decided to test a few theories. One worked. I will be submitting an article when I get out. Every time they take something from me, I gain more.

I am enclosing something your readers may find interesting. I by no means am trying to get hackers (locked up or otherwise) to hide. Never. But we are being classified as dangerous - hence, the 23 hours locked down, next to inmates who strangled 11 people.

I only have one more issue left on my subscription. It was a good test to see if I could get it. And I encourage all hackers to explore their environment.

Never underestimate the power of the right word and a smile.

Twenty Six Hundred
(apparently, this is my name)

The item you enclosed indeed referred to you by that name. It seems that you can earn that handle in prison simply by reading our magazine. Let's hope you never have to experience any more of their unique way of thinking.

Questions

Dear *2600*:

Can I use the *Off The Hook* audio on my website? I am wanting to add an audio player so my visitors can listen to the shows.

Bryan

We encourage this sort of thing. We just ask that you also point people to the source of the material. If you have access to a broadcast facility of any sort, we also encourage simulcasts or rebroadcasts so that even more people get sucked in.

Dear *2600*:

Strange subject I'm sure, but I'd guess you've seen worse. My question is, I would like to find a good community of tinkerers/hackers to talk with and perhaps even a good IRC or two. I never seem to be able to find channels with people actually talking. Do you guys have any advice for someone who just realized that he is a hacker (the learning meaning, not the cracker) at heart who just needs a little guidance? Thanks, even if this kind of question annoys you.

false

Well, the word "cracker" annoys us because it's such a meaningless term that's designed to foster suspicion and elitism. But we welcome questions of all sorts. You simply have to look around a bit and take some chances by wandering into forums, channels, and real-life 2600 meetings. You may not find what you're looking for right away, but do keep trying. You may also find positive things that you didn't know you were looking for. Nothing is predictable in our world.

Dear *2600*:

I am a 13-year-old with some skill in computers. I picked up your Winter issue (27:4), and I loved seeing all of the information in there. However, while reading it, it occurred to me: what is a hacker? I used Google and searched it, and I came up with www.catb.org/~esr/faqs/hacker-howto.html as the first result. However, that didn't seem to properly embody what your magazine described. Interestingly, *2600* is mentioned in the article as a way to "get ready to do five to ten in the slammer."

So, getting to the point, what is the "hacker" that *2600* talks about, and how is it different from the one Mr. Raymond talks about? Are they the same thing interpreted in different ways? What does a hacker do? The people of *2600* are described as "crackers." What is the difference here?

I hope I have not forced you to repeat something you have answered before (no doubt you receive many "Can you teach me to be a hacker?" letters to your magazine).

Anonymous

Actually, the "2600" mentioned in that piece is an unmoderated Usenet newsgroup called alt.2600 that really has no affiliation with us or with hackers in general. It once did, but with no oversight or standards, this newsgroup sadly fell into disrepair and disarray. We encourage you to read through it and then read through the material in our issues to see the difference. There are a lot of naive generalizations in the article you cite, which is unfortunate as it does seem to grasp the spirit of hacking for the most part. Definitions are always open to interpretation and to change, but to define yourself as the epitome of a "real hacker" and everyone else as some other word is basically closing off the discus-

sion. We need to avoid that trap.

Dear *2600:*

Your magazine's perseverance continues to amaze me. I find myself trying to collect the now "defunct" printed hacker magazines on eBay when I can find them. I don't think that I will ever have to track any *2600* issues down in the future - they will always be around. Congratulations on this amazing feat. Your magazine is a fantastic history lesson to the birth of the modern communication age with various perspectives told from both sides of the wire.

One thing I want to ask about, though, are the *2600* covers. I don't see many requests from the readers to the staff regarding the cover art. The *2600* covers have been overlooked since 1987. We need to change this ASAP, if not sooner. Every now and then, there is a mention of the covers in the letters, but not very often. I want to know about all of the hidden meanings in each of the covers from the random micro text in the background to the main image on the page. Sometimes I think I can decipher the general meaning of the covers, but other times I know there is a lot more going on than what meets the eye. It's like a *MAD Magazine* cover for us nerds. I think there is more work that goes into the covers than into most of the articles. I didn't even realize that on 26:1, it was an AT&T logo on the baby's shirt until Darth Vader pointed it out to me. In your early covers (the hand drawn ones), there are all kinds of micro text hidden away. I would inspect the covers with a jeweler's loupe as if I was inspecting a two carat diamond for flaws (I still do this on new covers). Also, in the early hand drawn covers, there was a space in the upper right hand corner of some random text or an image. I would really like to know all of the hidden eggs in each of these covers along with the meanings. The cover is one of the most interesting aspects of your magazine. On the back of your early issues, there was very small text at the bottom that said something like "It never happened" or "missing words." Please give us all some insight on all of these little things.

On your website, it says "As this site grows, we'll be adding explanations of each cover as well as selected highlights from our past issues." It has said this for quite some time now. Please start adding these explanations before the meanings are lost along with the artist that created the cover.

I also just want to know more about how they are made. Do you make them in-house or are they submitted by readers? Are they made as a collaborative effort by all of the staff at *2600*? Is there an agreed upon message by the staff for each cover? Are they photoshopped or are they actual pictures? The covers that have equipment - are these photoshopped or is there someone who makes these random equipment props? I am sorry for all of the questions. I just love the attention to detail in every single *2600* cover. I wouldn't mind owning poster sized versions of these covers, either. I'm sure it would be costly, though, but something to think about.

Thank you all for the years of hard work and dedication. *2600* has populated my reading library with very interesting material.

DMUX

We certainly do want to fulfill that promise of explaining the many covers we've put out over the years. We can be pressured with more interest and discussion, as we're only human. The covers are all made in-house. Some of the photos are untouched while others are heavily manhandled. What's interesting is that most of the ones people assume are doctored aren't, and vice versa. It's great to know that people appreciate the work that goes into them - this is precisely why we continue to produce them.

Dear *2600:*

The old phone system you guys had way back in the day used to have an awesome sound file. When you would call it, it would ring and say, "The number you have reached is not in service. If you feel you have reached this message in error, please hold and a hacker will assist you shortly." I know I'm probably asking a lot, but is there any archive that I can get that file from? Or do you maybe have it to send?

m m

Actually, the recording said, "If you'd like to make a call, please hang up and try again. If you need help, stay on the line and a hacker will assist you shortly." We have a few more, all recorded with the "official" phone company lady's voice of the 1980s and 1990s. We'll see about tracking down the rest of them and posting them online. Thanks for reminding us that they existed.

Dear *2600:*

hey why dont you start putting the ads in your magazine online. so as i can purchase shit from your supporters. do eet faggot.

Lane

Yeah, you know how to win people over and speak in elegant prose to boot. Most of all, though, you're able to make us feel really good about doing things in a manner that makes you unhappy.

Dear *2600:*

Just wanted to know if you guys have ever done a report on HARRP. If so, where can I find this?

eb

To our knowledge, we don't have any articles on the High Frequency Active Auroral Research Program. According to their website (www.haarp.alaska.edu), the purpose of this program is to "further advance our knowledge of the physical and electrical properties of the Earth's ionosphere which can affect our military and civilian communication and navigation systems." Sounds like something we could find interesting if someone were to write a hacker-oriented piece on it.

Dear *2600:*

How should I answer when my long-term girlfriend's mom asks why I am reading a book about hackers? She is in her mid 40s and only uses the PC to browse Facebook. This is a situation I was recently presented with, but I sort of shrugged it off. Is it worth spending time trying to explain what hacking really is and the negatives of automatically grouping hackers with cybercriminals and identity thieves? With that being asked, I became familiar with *2600* around late 2008 (very latecomer, I know). I am a 24-year-old working in application development for "the man" at a large company with the same initials of a certain wizard that attends Hogwarts. I picked up my first copy of *2600* at Barnes and Noble and have been hooked ever since. I am lucky to have come across it then, because it is the last time I can remember frequenting a bookstore (I have been ordering copies every quarter online). Also, at the time I was supporting back-end functions for a yellow and black U.S. CDMA provider that doesn't brand everything with "V" (horrid company, but that's a different story that I will likely write up and send in one day). I read the first copy from cover to back cover in one sitting and was more excited than I could articulate (or that maybe my then non-techie girlfriend could understand at least). A few days later, I eagerly purchased a copy of *The Best of 2600* from Amazon. Even though I continued to read the new *2600* publications, somehow *The Best Of* ended up on a bookshelf until late 2010. I have been reading the book during free time on the weekends and just recently finished. For any new readers who aren't familiar, this is an excellent book for anyone interested in the history of hacking (via phone, computer, and numerous other hackable devices). I only wish I had picked it up sooner. I was familiar with the story of Kevin Mitnick when *The Art of Deception* was released, but thoroughly enjoyed reading about the story as it progressed from hacker perspectives. This was the first time I realized how much fun reading hacker stories can be. A small group of friends and I began exploring the networks and Linux during high school while working on the help desk supporting Windows 2000 and Exchange Server. The closest thing I ever did to hacking was using Knoppix to pull Sam files from Windows XP directories and then using l0phtcrack and SAMinside to obtain admin passwords (not "hacking" so much, but educational). Some of this was necessary and appropriate, but some of it was also for fun and we were lucky the IT teacher never caught on. I recently ordered and began reading *Dear Hacker* and am loving the letters to the editor. Lastly, I wanted to express how much I love reading the *2600* on my Kindle and will continue to subscribe to the ebook. Its 1:22 am ET on April 1st and I've been waiting and hoping the new *2600* syncs down to Kindle before I'm off to bed. Please keep up the great work.

MyOwnMinerva

We find it's always worth the effort to try and explain the concept of hacking to people. We often underestimate their ability to "get it." Be assured that those who wish to demonize us will not hesitate to instill fear in as many people as they can find. We need to do whatever we can to provide the antidote to this.

Dear *2600:*

What exactly happened to the website? Its 8 pm on a Friday and I just realized I missed this week's broadcast of *Off The Wall*. I went to the *2600* home page to download the mp3 to find that www.2600.com has a "seized" notice up. I am not sure why this happened, but I know that the feds are always out to get you. I noticed a tweet about the "Contents of Sarah Palin email hack obtained by *2600*" and also noticed that post is no longer up (even though I can get to other pages on the site - just not the home page). I just finished reading the Spring 2011 edition of *2600* and hope all is well.

MyOwnMinerva

Dear *2600:*

Fuck! Just realized it's April Fool's day. I'm the fool. Well played, *2600*.

MyOwnMinerva

Until next year....

Dear *2600:*

Do you care if I create a "*2600* United States" LinkedIn group? The group will be max privacy and accept invitations from anyone who applies. What do you think?

fives

We generally are open to such ideas, but we like to know what the goals are, how it will be maintained and protected, what the benefit to the community will be, how it will tie to the magazine, etc.

Dear *2600:*

I wanted to subscribe to *2600,* but I didn't want to send a check or money order. Can I send cash?

Eric

You can, but it's always risky.

Dear *2600:*

Every once in a while, I'll notice someone has a *2600* email address, like johndoe@2600.com. My question is how does one get one. I've been on and off reading *2600* for a *long* time and think it would be outright cool to have one. Is there some kind of epic feat one must do? A secret ritual at a lodge in upstate New York? Or a "beat in" like they have with the Crips and the Bloods? But, really, I unabashedly want one for my handle. Never hurts to ask, right?

Frank

We hope the answer doesn't hurt, either. 2600.com addresses aren't something we give out, except to people working on specific projects involving the magazine. There are some older accounts that predate this policy but they've been grandfathered in.

Wikileaks

Dear *2600:*

Wanna hear something funny?

The law firm that is prosecuting "GeoHot" for

his Sony PS3 jailbreak is Kilpatrick, Stockton (KS). In 2009, KS was the largest intellectual property law firm in the U.S., and maybe the world, so they are definitely Empire and not Jedi.

Anyway, I was watching tweets come across this morning and one said, basically, "Sweden's Assange-attack-lawyer is from the U.S.!" The lawyer's name was given as "Nils Vastberg" (NV). His law firm? You guessed it, Kilpatrick and Stockton. NV's profile (but not his name) on the KS web page was removed. I also found something in Google cache on "Spoke" (which is like LinkedIn), connecting NV and KS.

At the time, I had all of five minutes to examine some other leads. Try this: one of the public figures to maintain his call for the death penalty for Bradley Manning is a guy named "James P. Cain." Cain was a lawyer at KS for 20 years, then U.S. Ambassador to Denmark (right next to Sweden). Another lead had KS working on al-Qaeda detainee matters. KS also hired some ex-CIA people.

Am I making too much of this? Or should Assange's prosecutor not be so heavily connected to the U.S.? (The blog *Legal Schnauzer* also claims a law firm for the Assange accusers has CIA ties!)

Terry

These are all interesting facts, but a quick poll finds that nobody is really all that surprised by them.

Dear *2600:*

I am writing to express my concern at the media attention Julian Assange appears to have gleaned at the expense of Bradley Manning. I am 100 percent behind the disclosure of this information to the general public and, at the time, Wikileaks appeared to be the best platform to undertake such a high profile disclosure. However, I find it extremely distasteful to see one man appearing to be presenting himself as the "savior of free speech" while the person who actually did some good rots in a military prison.

Why on Earth is Julian involved in the equation when interaction with the press could be done anonymously or via proxies? I would also question if somehow he had something to gain from this method of disclosure, be it financial incentive, or fame, or whatever... after all, the "final decision" on document publication is still in his hands. Wouldn't editorial decisions be better made as a group without the power of veto?

Anyway, just my two cents from an alternative viewpoint and thank you for producing such a great magazine. Please also take a look at the OpenLeaks project as I really don't think it's getting the attention it deserves - www.openleaks.org.

M3d1c473d

It's all fine and good to act anonymously or through proxies when dealing with sensitive issues. But what we need at this point in time is someone to actually step forward and vigorously defend what this organization stands for. That involves being in the limelight to a degree, but the flipside of that is the fact that it's a potentially dangerous position to be in. This is why other people aren't exactly clamoring for the attention.

We don't see this as being at the expense of Bradley Manning in any sense. Wikileaks has never revealed the name of their source(s) and we believe they never will. This fact needs to be recognized because it's the basic premise under which the Wikileaks concept is based.

We're not going to explore the personality issues and conflicts that exist within any organization. We do know that it's detrimental for them to eclipse the actual story and major accomplishments that have been achieved over the past couple of years. It's even more damaging when multiple organizations that allegedly stand for the same thing spend most of their time trashing each other and trying to cast aspersions. It makes little sense, points attention away from the real issues that need to be confronted, and risks putting everyone involved in a dangerously weakened position. If it continues, those opposed to Wikileaks and its ilk won't have to lift a finger to get their way.

Dear *2600:*

All aspiring hackers believe, and rightly so, that electronic freedom is one of the fundamental liberties we should protect. However, we should keep in mind the relative place our activities occupy in the big scheme of things, and resist self-aggrandizement.

That's also true for high-profile revelations such as WikiLeaks. Are Assange and Manning the source of the Tunisian uprising, which itself was the detonator for the wave of rebellions that shook North Africa and the Middle East? It's questionable. WikiLeaks "revealed" that Tunisia's leader, Ben Ali, was corrupt. To the Tunisian public, it was like revealing that water is wet. Worth a few smirks, yes, but not riots.

The actual triggers were twofold. First, the price of food rose (and has kept rising) to the point where subsidized food distribution programs ran out of money, creating widespread discontentment. Far from being helpful and sympathetic, petty officials actually added to the pressure by obstructing small businesses and requiring bribes to do their job.

On Dec. 17, 2010, a few local Tunisian policemen raided a produce seller called Mohamed Bouazizi and confiscated his fruits and his scale. Moreover, a female inspector had slapped him publicly while he was resisting the confiscation. He pleaded to get his property back, from the local police, then from the governor, to no avail. Overcome with humiliation and deprived of a livelihood, Bouazizi walked to the governor's building, doused himself with paint thinner, and set himself on fire.

This highly symbolic suicide was the watershed event that led to the expression of accumulated frustration and anger, and finally toppled the regime. WikiLeaks? Not so much.

High tech served the rioters by providing fast, uncensored communication through cell phones. But this was the work of mainstream corporations, not hackers. You are absolutely right when you say that governments will now try to turn off cellular and Internet communications at the first sign of un-

rest. That's exactly what Gaddafi did in Libya.

Note a constant trend: Engineers (that is to say, hackers) create technology companies to bring information to people. Governments "regulate" the amount of freedom that these companies can provide. This should give pause to activists that see government regulation over tech firms as a silver bullet for all the world's troubles.

SysKoll

Regulation is definitely not a silver bullet, nor is it always a bad thing. In the end, it's about people power and how much they're willing to let the governments or corporations get away with. We're pretty sure that mainstream corporations didn't sell their products as tools to use in popular uprisings. The people figured out how to do that on their own, just as they figure out how to bypass restrictions placed on them by their rules or by the software itself. The mood that's established by such empowerment, as well as by the existence of sites that are dedicated to leaking important information, is what tends to change the game.

Dear *2600*:

Four days before the 2011 Canadian federal election, Wikileaks released 9731 cables relating to Canada that all seem to incriminate one single party, and no one else. While I'm not a fan of that party, this seems all kinds of wrong, and hardly in the true hacker spirit of freedom of information. After reviewing more of these cables than I can count, I really feel like someone is trying to push an opinion on me here.

Any chance they also publish statistics about the number of cables they decided *not* to release? I'm guessing no.

Polaris75

Without knowing the specifics as to how these cables were obtained, it's impossible to judge the intent of their release. It could be that the person(s) who submitted them did indeed have a political agenda and only leaked the ones they thought would further that end. It could also be that, for whatever reason, one party had more damning documents than another. If Wikileaks themselves held back on the release of certain cables because of a political agenda, it would indeed be an interesting story, but we see no evidence of this having happened here or in the past. Of course, it's impossible to see any evidence without knowing what was leaked, which was done anonymously and we all know Wikileaks isn't going to reveal their sources. We heard similar accusations last year regarding the large amounts of leaked documents that involved the United States as opposed to other countries. We agree with all of the critics who are clearly clamoring for more leaked documents. But somebody has to leak them from a variety of sources in order for a variety of sources to be represented.

Hiding the Hacker Instinct: Or, No Oppressor Strategy Can Be More Successful Than Training the Oppressed to Oppress Himself/Herself

by Phineas Phreak

I want to say at the start that I do not plan to get horribly technical in this article. Really, the security components that gave rise to this topic were pretty simple. They were childlike even, though somewhat effective. However, my main point here is not to drool over what I found out while I was playing around. What I am concerned with is the fact that I felt I had to hide what I was doing.

At the law office where I worked at one point, there was a two-sided hallway where the elevators to our floor let off. The office was arranged in a ring around this double-sided hallway. Doors could close and lock at both sides, though one side was open to the reception area during business hours. Thus, during business hours, after you got off the elevator, you either proceeded through the open doorway to the reception area where you had to state your business to be admitted or you had to get through the locked door at the other side of the hallway. To get through the locked door, you either had to scan a prox card or announce yourself to the receptionist to get buzzed through. After hours, the door on the reception side of the hallway was locked as well.

Now, the story was different if you were coming from the office to the elevator hallway. Obviously, if you came from the reception side during business hours you just walked through the open doorway. However, if you were coming through a locked door, it unlocked just as you reached for the door.

This interested me. I understood that it was perceived to be more convenient to have the doors unlock when someone inside wanted out, but I was curious how this had been arranged. I'm sure the setup was not novel, but I was still curious. Was it a proximity sensor? Did the metal handle electromagnetically sense human touch on the inside handle? I wanted to know. I wanted to know how it worked.

I noticed that I heard a click anytime I approached one of the locked doors from the inside. One time when I was going through, I happened to look up and see a small white plastic box with something that looked like a sensor. Suddenly, it all made sense. Motion detectors. Motion detectors were mounted on the ceiling on the inside of each doorway, pointed to see someone inside the office approach the door on their way out into the elevator hallway. Quite simply, the detector detected motion and unlocked the door.

This revelation pleased me far more than it should have. It really was not that hard to discover,

but it still made me happy that I figured it out. Of course, it also got me thinking. The doors, though much sturdier than my doors at home, were still designed to be ornamental rather than secure. Though they locked fairly securely, there were significant gaps underneath and between the doors. Aesthetically pleasing as that may be, it also looked easy for someone to insert an object from the elevator hallway, through the gap under or between the doors, into the office. I thought it might be fairly easy to do so and trip the motion detector. It would have been fun for me to do so as a different way to get in instead of using my prox card, but someone else could do so as well. Someone who wasn't supposed to be in my office.

Really, I should have said something to someone. The office had a lot of computer equipment that someone might have found worth stealing, to say nothing of confidential client information. It was just too easy to get in. However, I said nothing. Reflecting on what I had been thinking, I further thought it would be bad for me if my firm knew that I thought in this way. I decided it would even be potentially dangerous for me to test my theory, under the possibility that someone might see me and know what I had been thinking. As a result, I stayed quiet and the flaw stayed in place.

However, I found out that I was not the only one. By chance, I learned that a coworker had been thinking similar thoughts. He had further noticed that a paper was delivered every day to the elevator hallway long before work hours. He imagined, and he actually had the gonads to test his imaginings when he had to come in really early one day before anyone else, that the paper could be used to open the door. Inserted fold down between the doors, the paper would fall open on the inner side of the door and trip the motion detector. Not only was the door locking system insecure, but also our firm provided the very object needed to circumvent it. Every morning.

This got me to the main point of this article, the idea that bugged me the most about all of this. Both my coworker and I had curiosity about the world around us, how things worked. Both of us examined our environment to see how the security doors functioned, how they might be circumvented, and how they could be made better. Further, we both - as our first gut reflex - automatically assumed that things would go badly for us if anyone found out. Neither of us, completely independently, was willing to make a peep in order that the doors could be made secure.

To me, this is the truly horrible thing about the whole situation. We did not even need to be punished for curiosity in order to understand that we needed to hide it. Instinctively, we understood. We knew what would happen and we knew it would not be good. No one even needed to tell us.

How could censorship of thought possibly function any better? Our firm, our corporate society, our government needed to do absolutely nothing. They did not have to act to crush resistance, because no resistance would be offered. We oppressed ourselves. As much of an individual as I like to consider myself, my own mind imprisoned me without any involvement of anyone in charge.

I think this is one of the most dangerous aspects of where our society has gone. We have been trained to punish ourselves, to keep ourselves in line. How much longer before our brains check those curiosity impulses before they even reach the level of conscious thought? The idea is frightening. The trend is frightening. And, worse, I'm not sure after seeing how I behaved in this circumstance that I will be brave enough to do anything about the situation. Hopefully, there are others braver than me.

Starting a Path to Modern Database Privacy

by Barrett Brown

Privacy has always been of interest to hackers. Firstly because back in the day all the coolest/funniest/most-interesting information was kept private and getting a hold of it was often an "Elite Hack." It didn't matter whether one social engineered the information or rooted a server from halfway around the world to get it: Excitement came from the fact that one had access to something that very few others did, something special, as well as the fact that "something" often directed the hacker to even more secret information that they could play with and which could potentially lead them to even more.

The second reason privacy was so important was due to the fact that the "first" so-labeled computer/phone/network hackers (I still consider Alan Turing a computer/network hacker for example, but in this article I'm referring mainly to the period from 1970 to the present) were engaging in activities that existed in a gray area of law. No precedents had yet been made by the Supreme Court about information theft by way of computer. So it was vital to many of those engaged in such activities to keep their "true identity" as secret as possible, the better to fight off any court cases should they one day occur, and thus came the origin of using a hacker "nick" or "handle."

Besides such logical purposes, privacy was (and is) a fundamental part of hacker culture specifically and Internet culture in general. Some sociologists think that this "privacy" is one of the biggest attractions to using the Internet for personal use. Instead of showing your face at the liquor store and blushing to the clerk because of the porn you just bought - well, presto, go to a web page! No one will ever know! Simply the act of logging onto a chat site

is a small example of this. You can choose to say whatever you like about yourself online. Change your race, age, whatever. As long as you have the acting ability to back it up, as far as anyone online knows, you are who you say you are. If you don't know someone in RL (Real Life), you either have to trust what they say online, on social networking sites, etc., or spend years and years chatting with them online, getting to know them, paying attention to everything they say, and eventually you may very well get a good idea of who they are.

How can an unknown (in RL) hacker with a nick trust another one whom they only know online? How do they know this new hacker they have been chatting up on IRC for months is not a federal agent trying to get the hacker thrown in jail? These are important questions because many a hacker has been caught in just this way: online communication only.

Well, in the old days (I'm an old-ish person), hackers would get on a BBS and trade information with each other. If the teleconference number, credit card numbers, or whatever "private" information that was being traded was good, the hacker's reliability rating went up, kinda like eBay ratings.

Because almost everything was private back in the day, hackers relied on war dialing, reading old manuals found in a CO (Central Office) dumpsters, social engineering telephone linemen and operators, and any other tactic a brilliant and motivated individual could come up with. But most important of all? Mutual collaboration. Without multiple people/groups working on similar puzzles independently and from different perspectives, then sharing the information found with each other through BBSes, text files, *Phrack, 2600,* other small groups working together, etc... well, we simply never would have had all the hacking successes that came throughout that time period. Why did total strangers who had often never met, talked on the phone, or knew anything about their partners in what would one day be deemed a "crime," decide to work with each other? Why did they often trade information that could get them put in prison for theft, treason, industrial espionage, or worse, get them a job at the CIA?

Privacy and Curiosity

Without the unwritten promise that those early hackers were "safe," that they were "private," hiding behind their computer screens, sometimes thousands of miles away from the computer(s) they were accessing (the extra-competent even routing their activities through tens of computers and different networks to add security), that even if their accomplices were caught, those accomplices had nothing but a nick.

These were some of the elements that made old-school hacking so exciting and gave people the freedom to explore the digital world to their heart's content. We "white hats" were freeing and sharing information, liberating it from those who wanted to control it and keep it from the public. Information was meant to be free and being a hacker meant that you were one of the freedom fighters in the battle.

Despite such democratic beginnings, the Secret Service's Operation Sundevil soon came along and, by getting hackers who actually did know each other to turn on their friends and associates, the Secret Service began the ruination of "hacker groups" and mutual collaboration. So began the cyber-age of hacker lone-wolves, larger international criminal cyber-theft rings, and the obvious need for even more privacy than before.

It's 2011 now and things have changed quite a bit. "Private Information," once the main purview solely of governments, private detectives, journalists, spies, and hackers is now big business. Where LexisNexis was once "The Database" used by all these people to find out anything about anyone, now there are *countless* data brokers out there, each one with their own specialty areas, each one trying everything in their power to find out everything they can about everyone and cross reference it. This means you. One hundred years ago, if you wanted to disappear, you just moved across the country, gave everyone in your new town a fake name and past, and you were pretty good to go. No national fingerprint databases, no genetic vaults cataloguing DNA, no satellites, no credit cards, no cell phone towers to silently inform people where/when you are, etc.

To summarize my introduction and get to the meat of my article: Maintaining one's privacy (particularly in America) these days is a daunting task. But for any good hacker, the harder the climb, the greater the reward. I am no criminal, I owe no large debts, I'm not skipping out on alimony, and there is nothing I am running from. I am simply a very serious believer in the intentions behind the writers of the U.S. Constitution, when they deliberated and thought very hard about the "God given right" that everyone has for reasonable privacy. Watching that privacy being eroded (maybe avalanching at this point?) year after year has inspired me to make a hobby of seeing just how invisible I can be.

So I bring to you, *2600* readers, straight from my own "privacy journal," some first steps in clearing up your digital footprint, along with notes I took along the way. Everything in this article I have performed and can personally vouch for. It is far from complete. Many books have written on the subject and society at large is far from achieving any reasonable kind of privacy (as the U.S. government and international data brokers continue to actively work toward breaking existing privacy laws) and I didn't get into changing Social Security numbers/names, filing off fingerprints, making an identity from scratch, flooding the databases with too much information to obscure what is real, or any other uber-advanced techniques.

Here I simply have a record of addresses, dates,

phone numbers, and procedures for the largest data brokers and government privacy agencies I could find, which anyone may use to increase their privacy. Enjoy!

LexisNexis

https://www.lexisnexis.com/➥opt-out-public-facing-products/

a) 7.17.10: Filled out LexisNexis online opt-out form. Saved reference number.

b) Printed out corresponding paperwork to be mailed or faxed.

c) LexisNexis has a very strict policy about removal of information. You must be a target of stalking or fit some other qualification listed on their site. You must prove it by supplying a police report, letter from a Social Services agency, or other proof. You must also send them a copy of two valid forms of ID, a list of all the places you've lived in the past ten years, a utility bill, and more.

d) I went to my local police station and retrieved a copy of an arrest that led to nothing from many years ago. In my letter to LexisNexis, I told them I was worried that the police in my case were "dirty cops" and that they would seek revenge on me because they lost their case (hey, it's possible...). I think I also used the word "attorney" a few times for good measure.

e) Mailed paperwork "certified mail," so I could prove they got it.

f) Emailed: privacy@lexisnexis.com requesting confirmation.

g) Received verbal confirmation of opt-out, waiting for paper receipt (two to four weeks, they said).

h) 8.21.10: Received mail from LexisNexis dated 7.17.10 denying my opt-out request, with no specific reason given. Saved paper in file. To succeed, I must: "Prove that [I am] an individual at risk of physical harm, or call LexisNexis privacy hotline at 800-831-2578 or LexisNexis privacy coordinator at 800-227-9597, extension 55568."

i) 8.22.10: Left a message for privacy coordinator.

j) 8.23.10: Received voice message from the privacy coordinator informing me that my opt-out order was actually approved, it's just that my mail got "crossed." Yeah, right.

k) Called privacy coordinator back and requested paper or email confirmation of opt-out.

l) 8.24.10: Privacy coordinator left voice message saying documentation is in the mail, ETA one week.

m) 10.1.10: Paperwork received and framed on my wall.

ChoicePoint

http://www.privacyatchoicepoint➥.com/optout_ext.html#optout

a) Filled out ChoicePoint opt-out form.

b) Received email confirmation.

c) Emailed copy of confirmation to my "records" email account.

Do Not Call List

https://www.donotcall.gov/➥register/reg.aspx

a) This is the U.S. government's "Do Not Call List" created a few years ago through an act of Congress. Although it feels good to have all my numbers on the list so I can threaten telemarketers (it works!), don't get too excited or put too much faith in it as any corporation can buy this list to use - and they do.

b) Registered all of my numbers.

c) Emailed copy of confirmation to my "records" email account.

The DMA (Direct Marketing Association)

http://www.ims-dm.com/

a) Many pages direct you here to get off of mailing/email lists.

b) Emailed privacy@the-dma.org asking about removal.

c) Directed to http://www.ims-dm.com/ for privacy.

d) Filled out forms in upper right-hand corner of page.

Intelius

https://www.intelius.com/➥privacy.php

a) Oddly, when I searched http://switch➥board.intelius.com/optout.php for my info, I couldn't find anything, so I thought I was not in the Intelius database. It was only after more research that I discovered I was.

b) 7.19.10: Faxed Intelius data brokers at 425-974-6194 my California ID with picture and number crossed out as directed, got fax confirmation, and filed it in paper records.

c) Emailed them requesting fax confirmation. Still waiting....

Acxiom

http://www.acxiom.com

a) Filled out remove request form (then waited for mail confirmation): http://www.acxiom.com➥/about_us/privacy/consumer_info➥rmation/opt_out_request_form➥/Pages/Opt-OutRequestForm.aspx

b) Requested "opt-out cookie" for targeted marketing: http://www.acxiom.com/prod➥ucts_and_services/TargetedEngage➥ment/DisplayAds/Pages/Relevance-➥XOpt-Out.aspx

c) 8.20.10: Received mail packet from Acxiom which included a mostly useless "Privacy Guide" with reference number which contained the "final opt-out form" which I mailed back promptly. Still waiting on final reply....

Google Phone Directory

http://www.google.com/help/pbremoval.html

a) Removed all numbers found.

whitepages.com

http://www.whitepages.com/myinfo/removal_form

a) Found my listing and removed it online.

Peoplefinder/Enformation

support@enformation.com

a) 7.19.10: Received Peoplefinder email back asking for a post letter, saying it will take five to six weeks....

b) Printed Peoplefinder/Enformation letter and mailed it: Opt-Out/Peoplefinders.com, 1821 Q Street, Sacramento, CA 95811. (Oddly, this address is used for more than two data broker businesses.)

c) Emailed them asking for confirmation when letter arrives. Still waiting....

Abacus

optout@abacus-us.com

a) 7.19.10: Emailed opt-out request.

b) 7.25.10: Received email from abacus optout@epsilon.com saying: "Per your request, we have suppressed your name and current address from Epsilon's Abacus Cooperative database. In addition, your name and current address will be blocked from entering our system in the future. Should you change your name or address, you may need to opt-out from Epsilon's Abacus Cooperative database again using your updated information."

c) Easiest to remove and most impressive response on record.

Random Magazines?

Everything was going so well until I got some magazines in the mail. WTF? After all my privacy work, I get catalogs?

a) Received an REI camping catalog in the mail with a code number on the label. I have never ordered from the company, do not camp, thought my mailing address was super-secret, and did not know how I got on their mailing list. I called their "mailing list removal number" (800-426-4840) and requested removal. They asked for my code number, then said they had removed me. Before hanging up, I asked them where they got my name and address. They had to check, but they found that they got my info from Title Nine, a clothing company I ordered two small items from several years ago who must have been actively stalking my change of address requests or getting my information from somewhere else.

b) Called Title Nine customer service (800-342-4448), gave them my customer number (on the catalog), and asked to be removed from their and all other databases. They said that it may take some time for the removal to be processed, but they will. Also I emailed remove@titlenine.com to be removed from their database completely, for good measure.

c) I should have known better, but this was the first I'd heard of magazines I order from passing around my address (even though I'd had about six changes of address since ordering from them) and it bugged me.

Email Opt-Outs and Other

From "Privacy-Alerts"

support@ameridex.com
remove@aristotle.com
customerservice@peopledata.com
webmaster@switchboard.com
http://www.infousa.com/
http://www.zoominfo.com/

Conclusion

In the end, this is just the tip of the iceberg. It's a full time job just trying to keep oneself out of today's information databases. Even after being cleaned from all the systems listed here, there are still credit reporting agencies, governments, Facebook, Gmail, hardware MAC addresses, and entities that will not erase your data no matter how nicely you ask.

In today's world, the only real privacy is not existing at all (or acting like you don't) and that's the best advice I can give to anyone who wants "real" privacy. Use Tor, OTR, encryption, and the countless decent plug-ins for Firefox to help make your identity less obvious. When filling out forms, if convenient, make a habit of transposing numbers/letters, so that in every database you are in your date of birth or name is just a little bit different. If you are doing something private, use one-way blind email, or even better *no* email. Boot your computer with a live CD operating system. Change your MAC address before logging onto any networks. Do anything and everything to stay private, not because it's cool or because of paranoia, but because it's our right as human beings. A right that we are losing minute by minute, a right that we will lose, if we don't stand up for it.

No matter how invasive the world becomes, there is always a way to fight fire with water.

Links

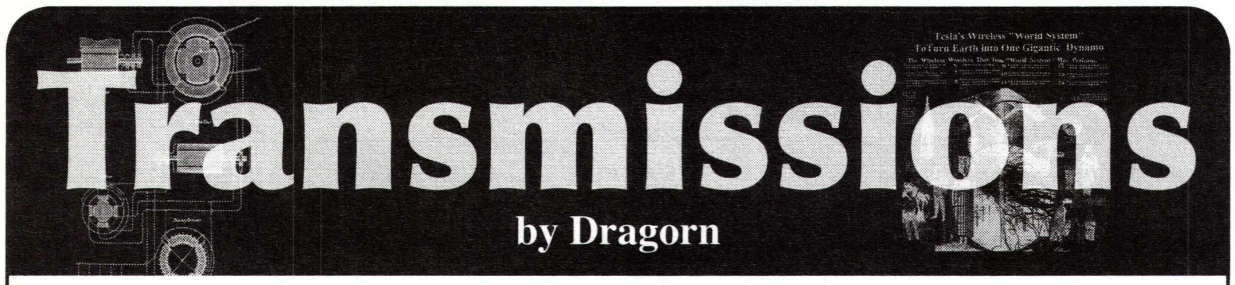
http://barrett.chaosnet.org/foxext/ - some good Firefox privacy extensions

http://www.haltabuse.org/ - site about fighting online stalkers

http://www.privacyalerts.org/ - many links from here

http://www.fas.org/blog/secrecy/ - government secrecy project

http://store.2600.com/privisdeadge1.html - this article was inspired by Steve Rambam



Real "Cyberwar"

The news has been yelling at us about "cyberwar" for what, a decade? The wars of the future will be fought with "computers" on "the Internet." I think I saw an episode of *SeaQuest* with this in the early 90s, right when the show got *really* crappy and time-travely.

The idea that some poor suckers we're carpet bombing will DDoS Amazon and keep me from ordering my sample of Uranium (seriously, go look it up) may be annoying, but isn't particularly frightening. Anonymous didn't manage to take Amazon out (though they did manage to make life highly annoying for a lot of other companies), and I'm fairly sure most of the countries we've decided not to share the playground with have less bandwidth available than the anonymous collective.

The typical tit-for-tat behavior of various hacker groups in feuding countries hacking the opponent's website and leaving the usual defamation messages isn't very interesting, either. There isn't any significant damage (besides that of pride) usually.

For things to get really interesting, we need to start looking at infrastructure-level attacks. "But," you cry, "No one would ever hook critical infrastructure up to the Internet. Surely, we know it's vital to insulate networks!"

Unfortunately, we don't learn. We're built by the lowest bidder, the cheapest contractor, the boss's nephew who needs a summer job. We love our Facebook, email, Twitter, Wikipedia, and office-time Bit Torrenting. It's so damn inconvenient to have to walk from the control workstation running the power plant, electrical grid, factory floor, etc., and go to the external system. It's such a pain not to be able to RDP directly into the management console to keep an eye on things from the road. And no one wants to pay for two workstations anyhow, right?

As we erode the air gap between critical infrastructure and the great unwashed Internet, we expose the infrastructure to greater and greater risk. The first shots have already been fired - Obviously, we can't ignore Stuxnet, but that's hardly the first case of extremely advanced attacks against infrastructure systems.

For example, in 2005, the voice switches for Vodaphone Greece were trojaned with an advanced, run-time patched piece of code, which tapped into the wiretap functionality to snoop on over a hundred government officials, company executives, embassy officials, and military officers. The perpetrators were never found: State actors? Organized crime groups? Suddenly, we're well beyond the purview of pranksters. (For an excellent complete chronology of the Greek phone hack, go read `http://spectrum.ieee.org/telecom/security/the-athens-affair`. We'll be here when you get back.) I don't know if this is the first publicly disclosed network attack against critical governmental services, but it's a very interesting data point.

Of course Stuxnet is still making news, a year after it was discovered, analyzed, debated, debated, fingers pointed, headlines made, debated further. Shockingly complex, specifically targeted, and subtly disruptive of a very specific piece of equipment, which just *happens* to be the heart of a hostile nation's nuclear program?

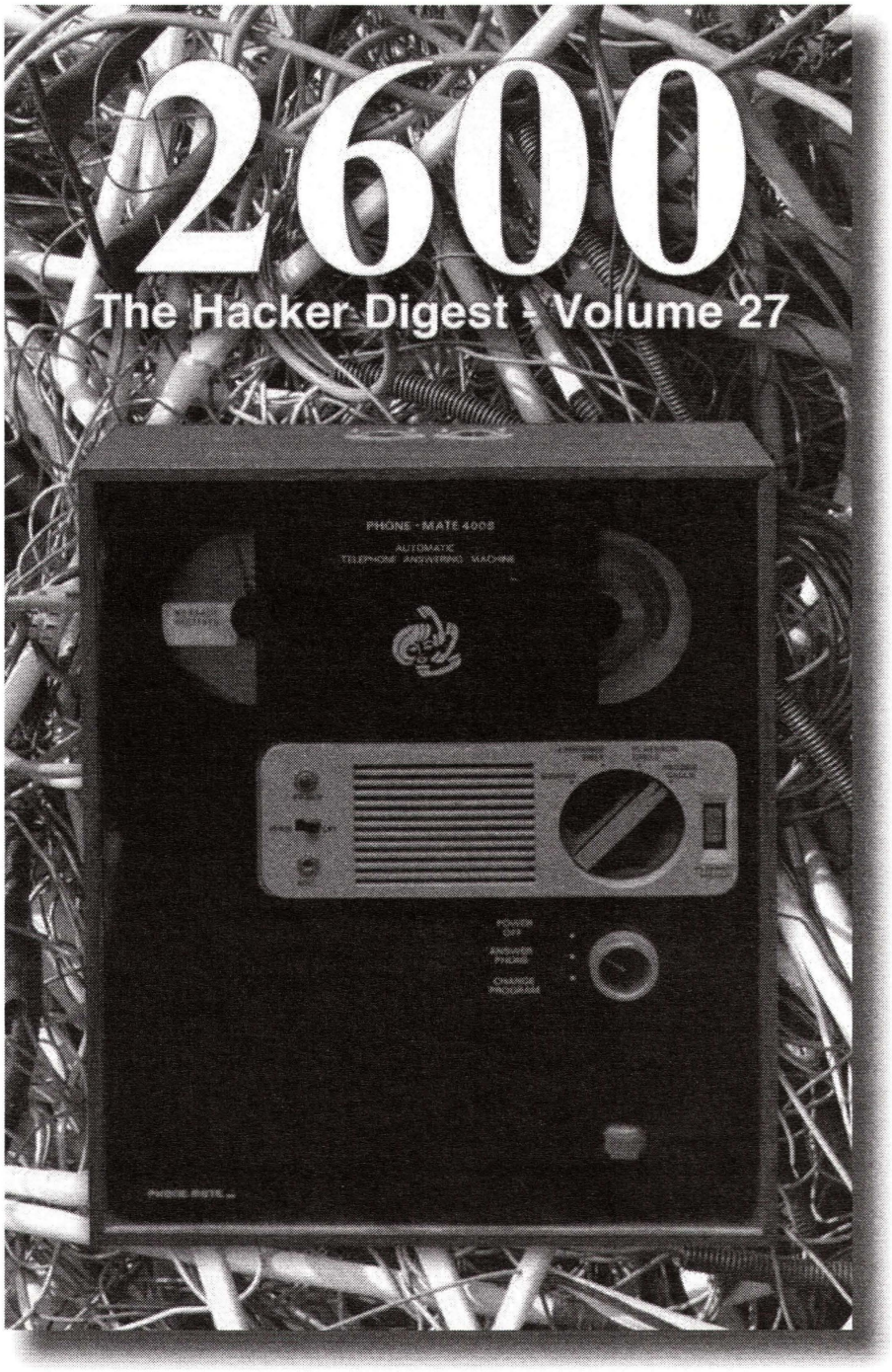
Iran blames the U.S. and Israel. The U.S. winks and says it's sure unfortunate for Iran, and isn't it such a shame. Israel is accused of building duplicates of the facilities in Iran for testing just such an attack.

No one is officially accepting ownership of Stuxnet. No one wants to be the ones to fire the first shot in a real, proper, "cyber attack." The real question left to me is: are we any more secure? I highly doubt it. Factories, power plants, even the "smart grid" being pushed by regional power companies use similar control systems, systems which were not necessarily designed to be hardened from external attacks. Some control systems likely predate the Internet and networks as we know them.

Changing software is fairly easy. Changing hardware is significantly less so. It's easy (for some relative definition of easy) to roll out a Windows patch on a Tuesday to close a hole, but when there are a thousand control systems over acres of a facility or hundreds of thousands of customers' homes, sharing a network where someone just brought a laptop back from the coffee shop, the next generation of specifically crafted worms may have a field day, and there's no simple way to change all those devices.

Siemens recently announced a group of vulnerabilities in its SCADA control systems which would not be publicly disclosed for reasons of national security; I have to wonder how similar they were to the same vulnerabilities Stuxnet was taking advantage of.

It's Here!



Now available online in PDF format
and for the Kindle and Nook!
All DRM-free, 275 pages

store.2600.com

A Brief Guide to Black Edition XP

by Oddacon T Ripper

If you don't remember, 9x was a term referring to the early versions of the Windows operating systems... 3.1, 95, 98... they were all 9x. It was called 9x because all of Microsoft's operating systems prior to it were eight bit operating systems. In the 1980s, most all computers ran eight bit OSes. MS-DOS, Apple II, GEOS, CP/M. were all popular back then. But when Microsoft released Windows 95, they designed it to support 32 bit! They would leave the processor at 16 bit for the sake of backwards compatibility, but Microsoft didn't change all of their code to 32 bit. This began to impact the operating system's efficiency and stability. Hence, the famous blue screen of death.

Microsoft has come a long way since 9x, though. With NT, XP, Vista, and Windows 7, they have overcome a lot of compatibility/networking issues. Can you sense the sarcasm? I remember when XP was first released on the market back at the turn of the millennium. It might as well have been called Swiss Cheese OS because there were so many security issues. One of the main exploits worked by booting XP using an older version of Windows and going into recovery mode. In older versions of Windows when you tried this, you were prompted to type in a password. But in Windows XP, this technique granted the "hacker" unrestricted access to the computer. The "hacker" then could access any of the files and folders on the system and copy them to any removable media. It didn't matter even if the system was password protected. Mostly, the issue was with holes in Microsoft programs. Remember the Melissa or the ILOVEYOU virus? They were both malicious worms geared for programs like Outlook, Word, Excel. Obviously, Microsoft answered by slowly pushing out updates - service packs, rather. SP1, SP2, and the almighty SP3, which featured some network security like NAP (Network Access Protection). Still, it was not enough. Remember in 26:3, "Microsoft, Please Salt My Hash!"? We found out that Microsoft wasn't even encrypting their passwords. This meant that stored passwords were not safe. So when a password got stored, there would be no way to encrypt or "hash" it. Salting is just a way of encrypting the passwords, which is a security feature UNIX systems have been using since the late 70s.

Black Edition

Windows XP accounts for over half of the consumer based operating systems out there today. So, if you're still running a 9x box, run Black Edition XP. First off, it's a copyrighted version of Microsoft's Windows XP, and that means it's illegal! So why bother running a pirated version of XP in the first place? Well consider that the original version of Windows XP had numerous security holes, as well as system and compatibility issues. I know what you're going to say: "I don't feel safe installing an OS that is not legitimate." Neither would I. If you're skeptical of viruses, trojans, becoming a botnet, and other malware, I suggest running Black Edition on a virtual machine. VirtualBox is a free program available at `http://www.virtualbox.org/`. If you have installed Black Edition XP on a different virtual machine, it will sometimes overwrite a config file called WINNT.SIF, resulting in the loss of the extra programs and custom settings. Worst of all, you will be asked to enter a key. If you have this problem, just use a key from the .txt file in the "\KEY CHANGER" directory on the disc/ISO. Then run "Auto Setup.bat" in the \OEM\RunOnce\ directory from the disc/ISO. After that, the custom setup will appear. However, you can also burn the ISO to a disc and format it like any other version of Windows XP. If, during the setup, you get a message that your hard drive is not detected or a blue screen pop-up, this usually means that the SATA driver for your hard drive is missing. Try to disable the SATA/ACHI option or set the SATA mode to IDE in your BIOS. If the setup starts, then install your SATA/ACHI driver, restart your computer, and change the BIOS hard drive setting back to SATA.

The setup process is similar to any other version of 9x, except that after it's finished, a custom message box prompt pops up with a 60 second warning that the preconfigured settings and extra programs will be installed, and, if nothing has been selected after 60 seconds, the option "Yes" will automatically be chosen. Then, a series of shell windows will pop up in dark green lettering, installing the various driver packs, runtimes, applications, patches, and updates.

After the shell-like DOS windows finish, the System Properties window will pop up and the ChaNinja theme will be defaulted along with a cool looking pirate skull background image. The language bar icon will also appear on the taskbar, defaulted to Luxembourg military time. Then suddenly, a dialog box will appear with a 30 second warning, saying that installation has finished and the computer will restart at the end of that duration. After the system reboots, everything should be working properly. You can remove the language bar by simply right clicking on the taskbar>Language Bar>Select Settings, clicking the Language Bar button, de-selecting "Show the language bar on the desktop" checkbox, and hitting the "OK" button. To change the time from Luxembourg military to another, click Control Panel>Regional and Language Options, then change the dropdown menu from "Luxembourgish (Luxembourg)" to your desired country.

While the identity of the group who disassembled the original Windows XP and assembled Black Edition XP remains unknown, rumors say that the group ORiON had something to do with compiling it. Anyway, Black Edition is an x86 32-bit version of XP that has been stripped of useless Microsoft components and pre-installed with a boatload of useful software. One important note about Black Edition is that it's an illegitimate version of Windows XP, so don't try to use your existing XP key. For one thing, it probably won't work. In addition, Black Edition XP comes with an XP key changer (Keyfinder) that registers Windows Genuine Advantage and removes the activation prompt. If you get a warning from your antivirus about this file, do not fret. All key generator programs are flagged as a virus.

Another noticeable feature of Black Edition XP is the boot time. This is due to certain files and programs that have been removed and certain updates that are slipstreamed in. Rest assured that anything that could create system problems or cause any software applications to crash has been removed. In fact, here is a list of the programs and components that have been removed: Address Book, Games, Internet Games, Paint, Pinball, Movie Maker, Music Samples, Old CDPlayer and Sound Recorder, Communication Tools, FrontPage Extensions, Internet Information Services (IIS), MSN Explorer, Netmeeting, Outlook Express, Windows Messenger, Blaster/Nachi Removal Tool, Desktop Cleanup Wizard, Out of Box Experience (OOBE), Security Center, Tour, Zip Folders, Display Adapters, and a few worthless directories and images.

Along with removing files, Black Edition has also integrated Service Pack 3 (SP3) along with all of the useful software. Remember that security issue I mentioned earlier about "salting the hash" and how Microsoft failed to address this flaw? Black Edition answered by integrating HashCheck Shell Extension (`http://code.➥kliu.org/hashcheck/`) which salts files and allows you to compare the checksums, letting you see if any data is corrupted. K-Lite Mega Codec has also been installed, along with Flash Player, QuickTime Alternative, Windows Media Player 11, DirectX, and Java SE Runtime Environment (JRE) to decode and encode almost all audio and video formats. Some other tools included are: 7-Zip (`http://www.7-➥zip.org/`), which has a high compression ratio compared to WinZip and supports 7z, ZIP, GZIP, BZIP2, ISO, RAR, TAR, and a bunch more extensions. DriverPack (`http://➥www.driverpacks.net/`) features hundreds of Chipset, CPU, GPU, Audio, Runtimes for ATI, Mass Storage, LAN, WLAN drivers. Chances are that DriverPack will not find every device driver in your system, and you will have to manually find some of the drivers on the web, so be aware of any devices that might not be well known or recognized.

Windows Internet Explorer 8 also comes defaulted with a bunch of cool links to online TV portals, various streaming music, underground searching databases, and open source programs like Notepad++ which has syntax highlighting for all you code junkies. Sandboxie isolates and secures web browsing. Daemon Tools is a virtual disk image emulator. OpenOffice is pretty much the number one open source alternative office program.

Since Black Edition XP is an underground project, there is no official source to download it or to seek further assistance from. It's sort of an open source, ongoing project with new updates and patches constantly being added, but you can easily find a copy of Black Edition XP by simply searching the web or by checking torrent sites.

THE MANY USES OF SSH TUNNELS

by twopointfour@riseup.net

SSH, as many of us know, is a protocol for remotely administering computers. You may hear people say "I'm gonna SSH into that box and restart apache" or something. As amazing as being able to remotely (and securely) connect to servers and run commands is, SSH can do a lot more than that. When you upload files securely with SFTP, you're actually using SSH to transfer the files. And SSH can also do some awesome port forwarding tricks. I'll just be talking about one type of port forwarding though: dynamic port forwarding. Dynamic port forwarding is turning an SSH server into a secure proxy server that your other applications can use.

You'll need access to an SSH server somewhere on the Internet for any of this to work. You normally get access to one if you pay for web hosting (with any halfway decent web hosting company anyway). You can pay a hosting company like Dreamhost $10 a month and they'll let you create as many SSH users on their server as you want, so you can give them out to your friends who are looking for an SSH server to tunnel through. If you have a computer that is always on at home, you can even set up your own SSH server. For the purpose of my examples, I'm going to assume that your SSH server's hostname is "myserver" and your username is "me".

You're also going to need some SSH software. If you're using Linux or a Mac, you already have it. If you're using Windows, you'll need to download it. There's a pretty good SSH client called PuTTY, but unfortunately it doesn't support dynamic tunnels. So instead, I suggest either installing SSH with Cygwin (`http://www.cygwin.com/`) if you know what you're doing, and, if you're not sure what you're doing, just use the OpenSSH Windows port (`http://sshwindows.sourceforge.net/`). You don't need to install the server, just the client.

Opening an SSH Tunnel

To create a SOCKS5 proxy server with SSH (aka an SSH tunnel), open up a command prompt and type this:

```
ssh -D 8080 me@myserver
```

This will SSH to myserver with the user me so you can run commands, and it will also start a SOCKS5 proxy server on localhost, port 8080 in the background.

Tunneling Firefox Traffic

Open up Firefox and download the add-on called FoxyProxy Basic. This add-on makes it easy to switch between proxy servers. After you restart Firefox, it should say "FoxyProxy: Disabled" in the bottom right of the browser. Right-click on that and select Options. Click the Add New Proxy button. A window will pop up with two tabs at the top, General and Proxy Details. Click the General tab and set the Proxy Name to be something like "ssh tunnel". Now click the Proxy Details tab and make sure the Manual Proxy Configuration radio button is selected. Under Host or IP Address put "localhost", and under Port put "8080". Check the box next to "SOCKS proxy?" and make sure the SOCKS v5 radio button is selected. Then click OK and close the FoxyProxy options. You have just added your SSH tunnel proxy to FoxyProxy.

Now you can right-click on FoxyProxy in the corner of your browser and switch between "Disabled" and "ssh tunnel". Go ahead and set it to "Disabled" for now, and go to a website like `http://displaymyip.com/` to see what the Internet thinks your IP address is. The IP address you see is your actual IP address. Now right-click on FoxyProxy and select "ssh tunnel", and refresh the page. If you opened your SSH tunnel correctly, it should now display a different IP address there, the IP address of your SSH server. Cool, huh?

So what's actually happening here? Since SSH connections are all encrypted, I'm going to use => to mean an encrypted SSH connection and -> to main a plaintext connection. The first thing you did was:

```
[home] -> [displaymyip.com]
```

And the website showed you your IP address. The second thing you did was:

```
[home] => [myserver] -> [display
➥myip.com]
```

This time, the website showed you myserver's IP address instead. And better than that, your connection between home and myserver is encrypted, which means if anyone is trying to eavesdrop on you at your local network, they can't see anything.

Now, on to the tricks.

Protecting Yourself on Public Wi-Fi

On open Wi-Fi networks (and many other networks too), it's trivial for an attacker to collect all the packets and look through them. You can use tools like aircrack-ng, wireshark, and FireSheep to do this. If you set Firefox to send all traffic through

your SSH tunnel, people can still try to monitor what you're doing, but all they'll see is a bunch of encrypted SSH traffic. No one will be able to sniff your traffic or hijack your sessions. They can even man-in-the-middle you if they want - it doesn't matter, they can't see what you're doing. They can even be sneaky and use tools like sslsniff to trick you out of using HTTPS, but it won't work.

Starting an SSH tunnel creates a local SOCKS5 proxy server, which means you can use several applications that support proxy servers, not just Firefox. You want to connect to your instant messaging server without people stealing your password? Pidgin and Adium support SOCKS5 proxies - check out your account settings. This works with most any email client, most any web browser, most any IRC client, and really most things that you do on the Internet. If you tunnel it all through SSH, eavesdroppers and attackers can't see what you're doing. (Also, people in IRC can't tell what your home IP address is.)

Getting Around Internet Censorship

A lot of networks block access to specific websites, like schools and particularly fascist businesses. A lot of governments have countrywide Internet censorship, like China, Australia, and, if the movie and music industries get their way, the United States and all of the countries in the European Union. If you're in this situation, you just need to connect to an SSH server outside of your censorship zone and tunnel your traffic through that. That's it.

So if you're in school and they won't let you connect to Facebook, tunnel your traffic through any random web host, and you can access Facebook through the tunnel. If you're in China and you can't look up information about Tibet, tunnel your traffic through the United States.

It's quite simple, and since it uses SSH instead of other plain text proxy servers, no one will be able to know what you're doing.

Infinite Megavideo Without Paying

If you've ever tried watching streaming pirated TV on the Internet (come on, we all have), you've probably noticed that most of the shows are hosted on random video hosting sites, and the most popular is `megavideo.com`. If you're watching a *Buffy the Vampire Slayer* marathon, you'll quickly notice that after 72 minutes (into S01E02), you get this error: "You have watched 72 minutes of video today. Please wait 54 minutes or click here to enjoy unlimited use of Megavideo." Annoying, right?

What it actually means is "your IP address has watched 72 minutes of video today." As soon as you get this error, you can right-click on FoxyProxy and switch from "Default" to "ssh tunnel" (thus switching to a different IP address) and refresh the page. This time, instead of coming from your home IP, you're coming from myserver's IP. Megavideo thinks you're a different user and you can continue watching without a problem. Until, of course, myserver has watched for 72 minutes. Then you can switch back to "Default" again, since it's been over 54 minutes.

Unlimited HTTPS With PdaNet Trial

PdaNet is an awesome smartphone Internet tethering app that lets you use your phone's data plan on your computer. You install the app on your smartphone, install another program on your computer, plug your phone in, and start the app. You can then connect to the Internet through your phone instead of with your wireless card. I've only used it on my Android phone, but there are versions of PdaNet available for iPhone, Blackberry, and Windows Mobile.

It comes with a free 30-day trial. It still works after that, but it blocks HTTPS websites. By default, SSH uses port 22, HTTP uses port 80, HTTPS uses port 443, etc. Technically, rather than blocking HTTPS, PdaNet actually just blocks all traffic going out on port 443.

But if you use an SSH tunnel, you'll be accessing port 80, 443, and possibly others, but only exiting your computer through port 22. So if you use PdaNet to connect to the Internet, start your SSH tunnel and set FoxyProxy to use "ssh tunnel", and none of your HTTPS traffic will get blocked.

PdaNet blocks connections that look like this because you would be connecting to port 443:

```
[laptop] -> [paypal.com]:443
```

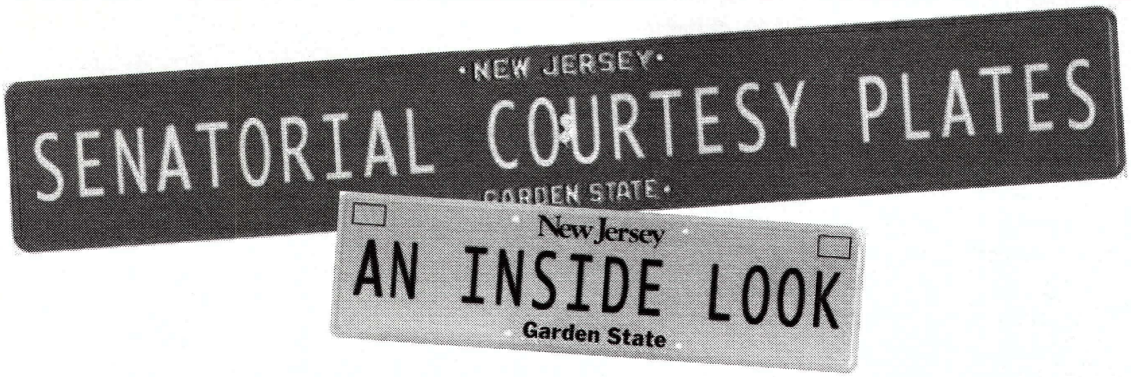
But they don't block these connections, because you're only connecting to port 22:

```
[laptop] => [myserver]:22 ->
➥ [google.com]:80
[laptop] => [myserver]:22 ->
➥ [paypal.com]:443
```

In Conclusion

To make things easier, you can set up passwordless SSHing with public key authentication (Google it). You can take the "ssh" command you run to open the tunnel and put it in a bash script so you don't have to type that whole thing each time (and you can modify it with -f -N so it just opens the tunnel in the background instead of opening a command prompt). You can even use something like autossh or a cron job to make sure your tunnel is always open, and then configure your applications to always use it.

Using an SSH tunnel encrypts your traffic locally, gives you another IP address to connect to servers with, and pushes all of your traffic through port 22 (or whatever port your SSH server is listening on). There are tons of other uses. Try it out.



by Dufu

I thought this might be interesting to some of the folks out there and also possibly stir up some additional conversation.

In New Jersey, there are license plates you can get for your car, truck, RV, or motorcycle that are called "Senatorial Courtesy Plates." Typically, they have three letters, then a space, and then a single number. If you go to the DMV with a custom plate request and have a three letter, single number combination, they will essentially turn you down on the spot because without Senatorial approval, you cannot own one of these plates in New Jersey.

Here is how the plate is useful to the local authorities or anyone else who might be interested:

The first letter is a "county" designation. For instance, "S" is for Somerset County. However, there are two other "S" counties. Salem is in the southern portion of the state and Sussex is in the north. Four counties start with "M" as well. Morris County uses the letter "L" and Middlesex uses "K," from what I understand. The numbers section is interesting as well with "6" and "7" typically reserved for people who are cops, although I know of at least a single person who was not a cop who had one. He did have some other high level government access, so I think they pulled some strings for him to drive around in his hot rod with "police plates," if you will. "1" is typically for Freeholders (county government officials) and very important mayors. I'd like to know how they determine VIP mayors from non-VIP mayors, but that's another story. "3," "4," and "5" are usually reserved for police chief use only.

I wish I had the full list of what all the letters and numbers mean, but this is all I could get out of my contact. Maybe someone else out there can write in with the information? Bueller? Bueller? Bueller?

Most of this information is supposedly not known at the local police force level except in large towns or cities, but it is well known at the state police level. Now you may wonder just how this would be useful to the Storm Troopers... er... I mean the New Jersey State Troopers. If you have one of these custom plates, they know where you are from by the first letter on your plate and who they might be stopping by the number. If a cop were to be following you and noticed your cool plate (as well as the fact that you were speeding or otherwise taking advantage of your crime permission ID tag), he or she knows before they pull you over how important of a person you are in the eyes of the government hierarchy. They can then make a decision prior to turning on their lights and sirens whether it will benefit them or be highly detrimental to their career path. This may shock and surprise a lot of you, but cops don't generally pull over other cops. Can you say legalized organized crime? An ex-girlfriend of mine had a father who was a Port Authority officer. He was a good man, but he told me of times when he would have to drive around in his old beat up pickup truck that could not pass inspection and was not registered. When pulled over, he would simply flash his badge and be sent on his way. That there, my friends is what these plates do for government officials, but it happens before and without the police stop.

<Mini Rant On> This is a little side note on the issue, but a friend of mine always says, "Never let intimidation or fear keep you from speaking the truth. Expose intimidation and banish fear! Exposure is sometimes the best form of accountability." To me, this is exactly the reason why this information has to get out there. Officers play a very important role in society and LEOs (Law Enforcement Officers) in general are a good thing. But as old farmer Brown used to say, one rotten apple can spoil the whole bushel, right? Those who were hired to "Serve and Protect" cannot be allowed to forget that little motto, even if it has disappeared from the side of most of their cruisers in the past few years. Those in office who were hired to serve and represent us seem to have forgotten that. They think we are here to serve them and their goals. *<Mini Rant Off>*

All of this information comes to me from someone who had a Somerset County plate back in the late 1980s, so it may be a bit outdated. He did, however, provide the information in December 2010, so I'm guessing that he would have added a little note about how things have changed if that was the case, since he keeps current contact with those in the government to this day.

I hope you enjoyed this little look into the workings of the New Jersey State Crime Allowance Organization. I'm sure it is similar to the CAO in your state or country as well.

by Suborbital
suboorbital@gmail.com (yep, two Ohs)

Squid (`www.squid-cache.org`) is an open-source proxy server that can be installed on any operating system. The configuration file is imposing, to say the least, but only because it contains basically the entire documentation for squid. Lines of default configuration file: 4984. Lines actually in use in my config file: 45. The squid instance described in this article was installed under the MacPorts package on OS X 10.6.something (although I have set it up under Windows XP, too).

I started out with the intention of blocking advertising on iPad applications. Normally, you could use something like the Firefox add-on "Ad Block Pro," but on an iPad, ads turn up all over the place, not just in web browsers (the Atomic Web Browser has ad blocking, but I was interested in things like ads in the BBC app). Fortunately, for a given wireless server, you can manually define a proxy, and so I duly set this to my MacBook, IP address 192.168.0.9, running squid on the default port, 3128. Squid was set up to allow proxying access to anything on the local (i.e., home) network, with the line

```
>> acl localnet src
➥ 192.168.0.0/16 # RFC1918
➥ possible internal network
```

and, most importantly, to log the terms in GET requests, with the line

```
>> strip_query_terms off
```

As an example, the request `http://www.google.com/search?q=2600` will be logged in its entirety, instead of just `http://www.google.com/search?`. POST requests are not handleable in the same way, but to examine the content of POST requests, you could probably redirect all traffic (at least temporarily) to a custom script whose only function was to enumerate POST request variables and their values. Secure requests (https requests, usually to port 443) are encrypted and also not available. On the whole, this is a good thing, as every request to `apple.com` was made via https, including some which look quite advertisement-seeking, such as

```
>> 1293720754.249 2663
➥ 192.168.0.10 TCP_MISS/200 1512
➥ CONNECT iadsdk.apple.com:443 -
➥ DIRECT/216.236.237.207 -
```

(the fields here (the squid default) being the timestamp, time to serve, requesting IP (i.e., the iPad), cache result (i.e., not found in cache), size of result (bytes), method (e.g., GET, CONNECT), URL address:port, the "hierarchy code" (rfc931), peerstatus/peerhost (i.e., how and where data was returned from), and returned data (MIME) type ("-" here, since it was not logged, but, e.g., "image/jpeg").

So, the ads being served through various apps were fairly easy to pick up, although there was one false positive (`tapjoyads.com`, used to authenticate purchases; the Wolfram Alpha app does the same). The ad servers that I saw in the squid access.log (which logs every request passing through squid along with whether it was served from the squid cache, a primary use of squid) were added to a blacklist file. This was included in the squid config file with the lines

```
>> include /opt/local/etc/squid/
➥blacklist.txt >> http_access
➥ deny BlackList
```

The blacklist.txt file contained a list of the servers to block, each one a regular expression, albeit trivial ones, like

```
acl BlackList url_regex -i
➥ google-analytics.com
acl BlackList url_regex -i
➥ googlesyndication.com
acl BlackList url_regex -i
➥ doubleclick.net
acl BlackList url_regex -i
➥ admob.com
acl BlackList url_regex -i
➥ ads.mp.mydas.mobi
acl BlackList url_regex -i google
➥_custom_search_watermark.gif
acl BlackList url_regex -i
➥ greystripe.com
...
```

The other servers currently in my blacklist are

```
iphone.playhaven.com
m.pinger.com
ads.pinger.com
serve.vdopia.com
www.fluik.com
www.jampaq.com
www.myprivatebrowserapp.com
analytics.medu.com
cloudfront.net
adwhirl.com
medialytics.com
imrworldwide.com
2mdn.net
```

Not all of these servers are ad servers per se, but some provide tracking of various kinds (e.g., `google-analytics.com`) and so were denied too. The `cloudfront.net` servers are used to provide content hosted on Amazon's cloud services and could conceivably serve up useful content, and so this regex might need some refining, but in all of the cases I saw, they were being used for ads. Seen in the logs but missing from this list was the server `tapjoyads.com`, used by the Doodle Buddy app, a free drawing application which contains themed sets of stencils, backgrounds, and stamps, to check for purchased sets (you get one free); it also contains banner ads, but these were served by `greystripe.com`. Note to developers: please don't use servers with the term "ads.com" in them for serving legitimate content. It's disingenuous. As another example, the BBC news app ads were served by `ad.mo.doubleclick.net`. All easily dealt with using the above blacklist; from their frequency, it appears that either greystripe, doubleclick, or admob are serving ads from the iAd system (Apple's in-app ad server), or perhaps more than one of these.

Of note is `www.myprivatebrowser.com`. This free web browser promises "a simple web browser built for the iPad that removes all your web browser cookies and history when you open and close the browser." Not all that secure, but better than nothing, right? Well, when you open it, the default (unchangeable) home page is a custom Google search form, which immediately runs off and requests `http://www.myprivate➥browserapp.com/app/big.gif`. Nice statistics gathering, Cooply Apps! Welcome to the blacklist!

So, ads come from all over the place (including the usual suspects), and (at least at home) you can set up a proxy to deal with them. What other strange requests are going out over the airwaves from your iDevice? Only your unique device identifier (UDID). Only to ad servers (well, not only). Requests were made to the following servers which passed my iPad's UDID in GET requests:

```
ads2.greystripe.com
adsx.greystripe.com
mayhem.eamobile.com
serve.vdopia.com/adserver/...
ws.tapjoyads.com
```

Gah! Well, `tapjoyads.com`, checking what in-app add-ons I'd purchased... okay. EA games (`eamobile.com`), seemingly informing them of in-game achievements... okay. But greystripe? WTF? And here's an interesting one (line breaks inserted before each GET variable; x's added for anonymity):

```
>> http://ads.mp.mydas.mobi/getAd
➥.php5?sdkapid=18754
&auid=b4585xxxxxxxxxxxxxxxxxxxx
➥xxxxxxxx23463
&mmisdk=3.5.8-10.6.29.i
&ua=iPad%204.2.1
&age=31
&vendor=adwhirl
&lat=0.000000
&zip=
&long=0.000000
&adtype=MMBannerAdBottom&hswd=728
&hsht=90
&accelerometer=true
```

Here we have a request to an ad server which uniquely identifies my iPad, passes my age (well, that's not mine, but perhaps I entered this one somewhere?), the version of my iPad's OS, whether I have an accelerometer in my device (or whether it's on?), and, although not used, *my latitude and longitude??* If this were a useful app that happened to start up with the request "App XXX would like to use your current location", perhaps those might have been passed on to the ad company. If anyone can find such an example, please write in. All in all, it was no surprise that, in the middle of this project, a story appeared on the BBC news app (ha!) about a class action against Apple for allowing personally identifying data (i.e., the UDID) to be shared unnecessarily and without users' consent.

It's 2011. Do you know where your ads are coming from? The converse might just be true.

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $100 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, email us at happenings@2600.com or by snail mail at Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA. We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker

July 30-31
Maker Faire Detroit
The Henry Ford
Dearborn, MI
makerfaire.com/detroit/2011/

August 4-7
Defcon
The Rio Hotel and Casino
Las Vegas, NV
www.defcon.org

August 5-7
NinjaCon
The Hub Vienna
Vienna, Austria
2011.ninjacon.net

August 10-14
Chaos Communication Camp
Finowfurt, Germany
events.ccc.de/category/camp-2011

August 26-27
JurackerFest 2011
Centre paroissial l'Avenir à Delémont
Delemont, Switzerland
blog.jurackerfest.ch

August 27-29
Large Hacker Space Convention
RaumZeitLabor
Mannheim, Germany
raumzeitlabor.de/wiki
/1._Large_Hackerspace_Convention_(LHC)

September 8-9
SEC-T
Nalen
Stockholm, Sweden
www.sec-t.org

September 17-18
Maker Faire NYC
New York Hall of Science
Flushing Meadows, NY
makerfaire.com/newyork/2011/

September 30-October 2
DerbyCon
Hyatt Regency
Louisville, KY
www.derbycon.com

December 27-30
Chaos Communication Congress
Berliner Congress Center
Berlin, Germany
events.ccc.de/category/28c3

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.

For Sale

CLUB MATE now available in the United States. The caffeinated German beverage is a huge hit at any hacker gathering. Available at $45 per 12 pack of half liter bottles. Bulk discounts for hacker spaces are quite significant. Write to contact@club-mate.us or order directly from store.2600.com.

CRYPTOCURRENCY AND DIGITAL CURRENCIES for sale or trade. Bitcoin, Pecunix, HD-Money, Liberty Reserve, c-gold, EuroGoldCash and more! NanaimoGold.com 604-628-6966.

DANGEROUSPROTOTYPES.COM. Hack your work with open source hardware. NEW: Bus Blaster v2 ($35) JTAG debugger - a reprogrammable, upgradable buffer makes it compatible with lots of applications. Get started in programmable logic with $15 CoolRunner-II and XC9572XL CPLD development boards - replace a bunch of 7400 series logic chips with your own custom IC. The Bus Pirate ($30) is a universal bus interface that talks to electronics from a PC serial terminal, save time working with new or unknown chips. Check out all our open source projects at DangerousPrototypes.com.

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Turning off TVs is fun! See why hackers and jammers all over the planet love TV-B-Gone. Don't be fooled by inferior fakes. Only the genuine TV-B-Gone remote controls can turn off almost any TV in the world! Only the genuine TV-B-Gone remote control has Stealth Mode and Instant Reactivation Feature! Only the genuine TV-B-Gone remote control has the power to get TVs at long range! Only the genuine TV-B-Gone remote control is made by people who are treated well and paid well. If it doesn't say Cornfield Electronics on it, it is not the real deal. Also available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! *2600* readers get the keychains for 10% discount by using coupon code: 2600REAL. www.TVBGone.com

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v28no2" and get 10% off of your order.

GAMBLING MACHINE JACKPOTTERS, portable magnetic stripe readers & writers, RFID reader writers, lockpicks, vending machine jackpotters, concealable blackjack card counting computers, computer devices, odometer programmers, and much more. www.hackershomepage.com.

CAPT'N CRUNCH WHISTLES. Only a few left. THIS IS *THE ORIGINAL* WHISTLE from Capt'n Crunch cereal box. Brand new, unused, mint condition! Join the elite few who own this treasure! Once the remaining few are sold, that's it - there will never, *ever,* be another one offered again. Key chain hole for easy insertion on your key ring. Identify yourself at meetings, etc. as a *2600* member by dangling your key chain and saying nothing. Cover one hole and produce *exactly* 2600 hz. to beep-off a long distance call so you can then Multi Freq. another if your telephone office uses in-channel long distance equipment. Cover the other hole and you get another frequency. Use both holes to call your dog, dolphin, concubine, or hamster. Also, ideal for telephone remote control of your own electronic remote devices. Price includes mailing. $79.95. Not only a rare collector's item but a VERY USEFUL and unique device which is easy to carry with you at all times; nobody will know, except you, how it is used! Cash/money order only. Mail to: WHISTLE, P.O. Box 410802 (ST), CC, Missouri 63141.

AT OWLDOMAIN.COM we take pride in helping our users develop and deploy their newest ideas. Need a VPS? How about a dedicated server? Maybe shared hosting? We have all of those and more! We realize the economy is in the gutter right now, Let us be the rope to help you get back on the top with packages starting as low as $4.95 USD a month. Did we mention unlimited bandwidth and data space with our shared hosting? OwlDomain completely supports *2600!* So much in fact that we have already cut our prices by over 26%!

Help Wanted

NO COMPROMISE PROVIDER of open architecture-based network privacy & security services is actively searching for exceptional technologists (of all hat colors) with extensive experience in network topology/ design, VPN architectures, and general *nix sysadmin - we recently survived a massive federal effort to shut us down via extralegal harassment & imprisonment of our founding CTO on political grounds; company is now bouncing back & expanding our service offerings (telecom included). Must have strong loyalty to principles of free expression, anti-censorship, genuine cultural diversity. Tribal-based management philosophy - strong financial performance, strong community involvement. Details, compensation info, & longtime community credentials available via: wrinko@hushmail.com. Namaste.

ATTN *2600* ELITE! In early stages of project to develop an international social network for information exchange. Just a few topics include: cryptography/secure communications, sovereignty, business and tax law manipulations, quantum causality, algorithmic structures, network traffic analysis, social engineering, and much more. Are you looking to apply your technical skill set to a multitude of world changing projects, or need to barter information with professionals to expand your reference base? We need your help to see this project succeed. For details write: Joseph Hayden #74101, L.C.F., PO Box 2, Lansing, KS 66043.

Wanted

PAYPHONE PICTURES & NUMBERS WANTED from around the world. Please send in pictures of payphones in unusual, famous, or interesting places, along with the payphone's callable telephone number where possible. Please send all to sfoswald+payphone@gmail.com, with as much information as possible. All contributions will be added to the increasing collection of callable international payphones. Miscellaneous payphone information is also welcome. The site is called PayPhoneBox and can be found via www.payphonebox.com.

SEEKING TELEPHONE EXCHANGE LOCATIONS. I want your lists of telephone exchanges, their locations, and the numbers and area they serve. Extra points for third-world countries. I am willing to pay with dollars or trade for similar data. Contact: BitRobber@shady.tel (pgp key fingerprint: 8BA9 5A91 2407 1DA6 6AC2 F9C2 04A8 C3D1 073D 9665).

Services

COMPUTER FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality computer forensics and electronic evidence support for criminal defense attorneys. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism and more. Sensei forensic technologists all hold prestigious forensics certifications. Our principals are co-authors of *The Electronic Evidence Handbook* (American Bar Association 2006) and of hundreds of articles on computer forensics and electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers and even *O* magazine. For more information, call us at 703-359-0700 or e-mail us at sensei@senseient.com.

JEAH.NET UNIX SHELLS & HOSTING. How about Quad 2.66GHZ processors, 9GB of RAM, and 25x the storage? JEAH.NET is #1 for fast, stable, and secure UNIX shell accounts. Use hundreds of IRC vhost domains and access all shell programs and compilers. JEAH also features rock-solid UNIX web hosting. *2600* readers' setup fees are always waived. We support *2600,* because we read too! Don't forget our free private WHOIS registration service, with domain purchase, at FYNE.COM.

PLEASE HIRE ME! I am a hacker in desperate need to break into the IT and infosec industry. I don't have certs, but loads and loads of experience. Resume and references available upon request. Sysadmin, VoIP admin, DBA, tech writing, ANYTHING please. Infoinject@gmail.com or 866-501-CHEN x007. Thank you in advance.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by Intelligent Hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without Big Brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

Announcements

WE LIVE IN AN INCREASING AGE OF MISINFORMATION, fraud, and dysfunction. We need more people exploring, collecting, and connecting public Intelligence in the public Interest (Cryptome.org, Wikileaks.org). I work as the NYC Director for the nonprofit Earth Intelligence Network. Our Online *Public Intelligence Journal* (*loaded* with resources) can be found at http://phibetaiota.net. We seek to identify dysfunction and energize creative solutions by interconnecting and harmonizing the 12 policy domains with the top 10 global threats and 8 challengers - http://is.gd/d0FOj Related links: twitter.com/earthintelnet, youtube.com/earthintelnet, www.earth-intelligence.net, true-cost.re-configure.org, smart-city.re-configure.org. Free books: Intelligence for Earth - http://is.gd/b4519 & Collective Intelligence - http://tr.im/jo9S Contact earthintelnet@gmail.com.

EXPLORE. COLLECT. CONNECT. Various FYI: public intelligence blog at phibetaiota.net, re-configure.org, true-cost.re-configure.org, webtxtmsg.com (make your web content accessible through text-messaging). For those in NYC, get subway updates by sending "txtnyc" (space) "subup" to 368-638 (DOTNET). This is part of my txtnyc mobile info service experiment. For more, just send "txtnyc" to 368-638. Contact: mobiledemocracy@hushmail.com

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and Central America at 5110 khz. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Shows from 1988-2010 are now available in DVD-R high fidelity audio for only $10 a year or $150 for a lifetime subscription. Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

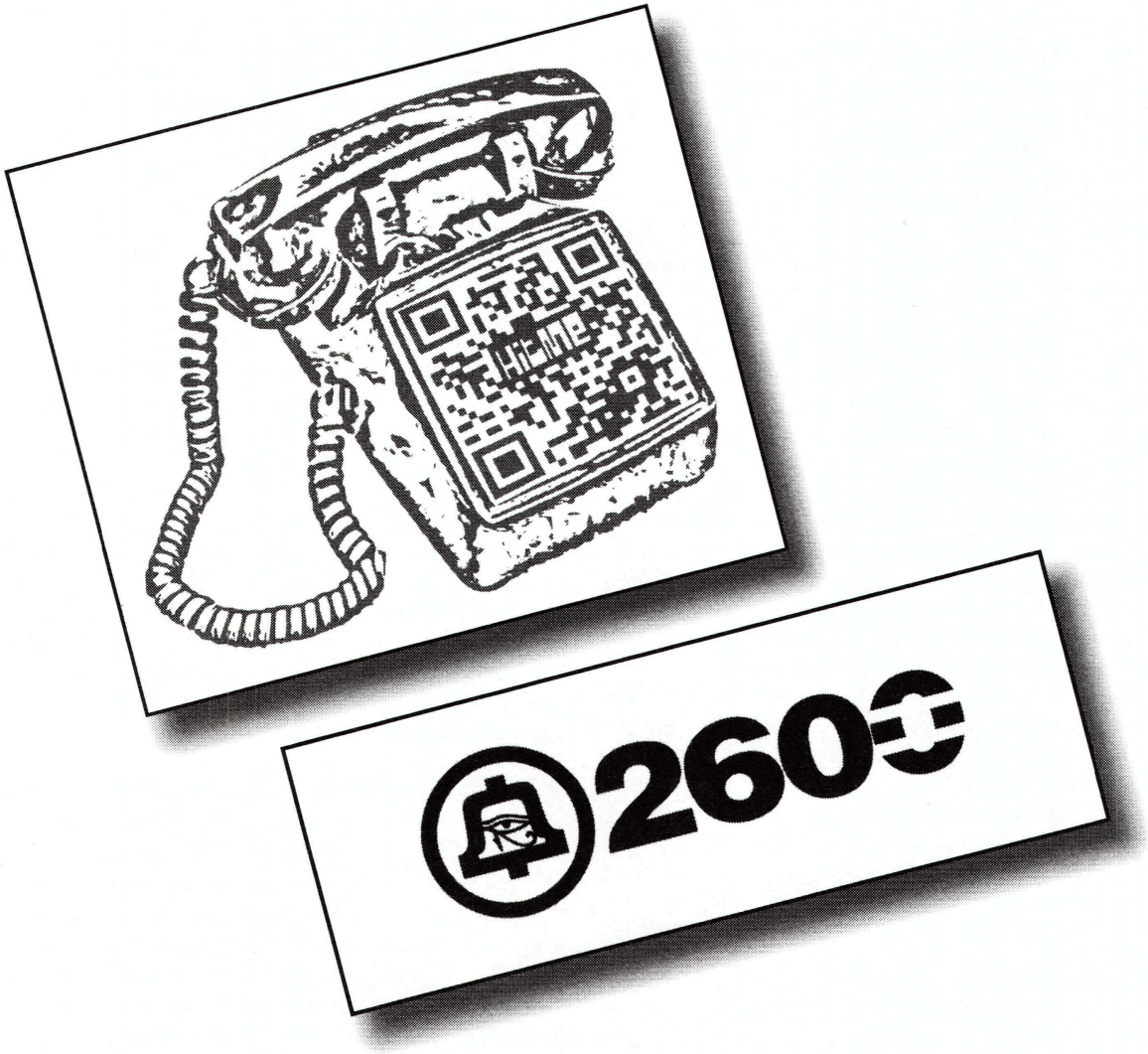
ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com. Be sure to include your subscriber coding (those numbers on the top of your mailing label) for verification.

Deadline for Autumn issue: 8/20/11.

NEW T-SHIRT!

This is anything but your typical hacker-chic barcode style t-shirt. We think our deskphone image (green in color) is both pleasing to the eye and useful in a pinch. The *2600* old-school telephone logo on the back (black in color) completes the mood. Shirts are 100% cotton and white, available in sizes S to XXXL.

$20 includes shipping, except overseas.



Find it at store.2600.com

or mail a check or money order to:

2600
PO Box 752
Middle Island, NY 11953 USA
(overseas, add $5.25)

"If journalism is good, it is controversial by its nature."
- Julian Assange

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

S T A F F

Infrastructure
flyko

Network Operations
css, phiber

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Forum Admins
Bunni3burn, dot.ret

Inspirational Music: Nusrat Fateh Ali Khan, Bright Eyes, Poison the Well, Johnny Horton, The New Pornographers, L'Arc-en-Ciel, Daft Punk, The High Strung, Michael Franti

Shout Outs: Daniel Ellsberg, Jacob Appelbaum, Harry Allen, Nick Jarecki

***2600* is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.**

2600 (ISSN 0749-3851, USPS # 003-176); Summer 2011, Volume 28 Issue 2, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. and Canada - $24 individual,
$50 corporate (U.S. Funds)
Overseas - $34 individual, $65 corporate

Back issues available for 1984-1986 at $10 per year, 1988-2000 at $2.50 per issue, 2001-2010 at $6.25 per issue. (1987 only available in full back issue sets.) Subject to availability. Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

Copyright © 2011; 2600 Enterprises Inc.

ARGENTINA
Buenos Aires: Rivadavia 2022 "La Pocilga."

AUSTRALIA
Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm
Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA
Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL
Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA
Alberta
Calgary: Eau Claire Market food court by the wi-fi hotspot. 6 pm
British Columbia
Kamloops: At Student St in Old Main in front of Tim Horton's, TRU campus.
Manitoba
Winnipeg: St. Vital Shopping Centre, food court by HMV.
New Brunswick
Moncton: Champlain Mall food court, near KFC. 7 pm
Newfoundland
St. John's: Memorial University Center Food Court (in front of the Dairy Queen).
Ontario
Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm
Toronto: Free Times Cafe, College and Spadina.
Windsor: Sandy's, 7120 Wyandotte St E. 6 pm
Quebec
Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere near the Dunkin Donuts in the glass paned area with tables.

CHINA
Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC
Prague: Legenda pub. 6 pm

DENMARK
Aalborg: Fast Eddie's pool hall.
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm

ENGLAND
Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm
Leeds: The Brewery Tap Leeds. 7 pm
London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm
Manchester: Bulls Head Pub on London Rd. 7:30 pm
Norwich: Old Borders entrance to Chapelfield Mall, under the big screen TV. 6 pm

FINLAND
Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE
Cannes: Palais des Festivals & des Congres la Croisette on the left side.
Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 9 pm
Paris: Quick Restaurant, Place de la Republique. 6 pm
Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm
Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 pm

GREECE
Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND
Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY
Milan: Piazza Loreto in front of McDonalds.

JAPAN
Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.
Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO
Chetumal: Food Court at La Plaza de Americas, right front near Italian food.
Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS
Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NEW ZEALAND
Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm
Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

NORWAY
Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm
Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm
Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU
Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

SOUTH AFRICA
Johannesburg (Sandton City): Sandton food court. 6:30 pm

SWEDEN
Stockholm: Central Station, second floor, inside the exit to Klarabergsviadukten above main hall.

SWITZERLAND
Lausanne: In front of the MacDo beside the train station. 7 pm

WALES
Ewloe: St. David's Hotel.

UNITED STATES
Alabama
Auburn: The student lounge upstairs in the Foy Union Building. 7 pm
Huntsville: Stanlieo's Sub Villa on Jordan Lane.
Arizona
Phoenix: Lola Coffee House, 4700 N Central Ave. 6 pm.
Prescott: Method Coffee, 3180 Willow Creek Rd.
Arkansas
Ft. Smith: Sweetbay Coffee, 7908 Rogers Ave. 6 pm
California
Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.
Monterey: Mucky Duck, 479 Alvarado St. 5:30 pm.
Sacramento: Round Table Pizza at 127 K St.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Plaza (inside). 5:30 pm
San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm
Tustin: Panera Bread, inside The District shopping center (corner of Jamboree and Barranca). 7 pm
Colorado
Colorado Springs: Barnes & Noble, Citadel Mall. 5:30 pm
Connecticut
Waterbury: Brass Mill Mall second floor food court. 6 pm
District of Columbia
Arlington: Champps Pentagon, 1201 S Joyce St (in Pentagon Row on the courtyard). 7 pm
Florida
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm
Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm
Orlando: Fashion Square Mall food court, 2nd floor.
Sebring: Lakeshore Mall food court, next to payphones.
Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm
Georgia
Atlanta: Lenox Mall food court. 7 pm
Hawaii
Hilo: Prince Kuhio Plaza food court.
Idaho
Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700.
Pocatello: Flipside Lounge, 117 S Main St. 6 pm
Illinois
Chicago: Golden Apple, 2971 N. Lincoln Ave. 6 pm
Indiana
Evansville: Barnes & Noble cafe at 624 S Green River Rd.
Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm
Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.
Iowa
Ames: Memorial Union Building food court at the Iowa State University.
Davenport: Co-Lab, 1033 E 53rd St.
Kansas
Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.
Wichita: Riverside Perk, 1144 Bitting Ave.
Louisiana
New Orleans: Z'otz Coffee House uptown at 8210 Oak St. 6 pm
Maine
Portland: Maine Mall by the bench at the food court door. 6 pm
Maryland
Baltimore: Barnes & Noble cafe at the Inner Harbor.
Massachusetts
Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm
Northampton: The Yellow Sofa, 24 Main St. 6 pm
Worcester: TESLA space - 97D Webster St.
Michigan
Ann Arbor: Starbucks in The Galleria on S University. 7 pm
Missouri
St. Louis: Arch Reactor Hacker Space, 2400 S Jefferson Ave.
Springfield: Borders Books and Music coffeeshop, 3300 S Glenstone Ave, one block south of Battlefield Mall. 5:30 pm
Montana
Helena: Hall beside OX at Lundy Center.
Nebraska
Omaha: Westroads Mall food court near south entrance, 100th and Dodge. 7 pm
Nevada
Las Vegas: Barnes & Noble Starbucks Coffee, 3860 Maryland Pkwy. 7 pm
Reno: Barnes & Noble Starbucks 5555 S. Virginia St.
New Mexico
Albuquerque: Quelab Hacker/MakerSpace, 1112 2nd St NW. 6 pm
New York
New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.
Rochester: Interlock Rochester, 1115 E Main St. 7:30 pm
North Carolina
Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm
Raleigh: Royal Bean coffee shop, 3801 Hillsborough St (next to the Playmakers Sports Bar and across from Meredith College).
North Dakota
Fargo: West Acres Mall food court by the Taco John's. 6 pm
Ohio
Cincinnati (Walnut Hills): The Brew House. 7 pm
Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd. 7 pm
Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm.
Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.
Oklahoma
Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.
Oregon
Portland: Theo's, 121 NW 5th Ave. 7 pm
Pennsylvania
Allentown: Panera Bread, 3100 W Tilghman St. 6 pm
Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm
Philadelphia: 30th St Station, southeast food court near mini post office.
Pittsburgh: Panera Bread on Blvd of the Allies near Pitt and CMU campuses. 7 pm
State College: in the HUB above the Sushi place on the Penn State campus.
Puerto Rico
San Juan: Plaza Las Americas by Borders on first floor.
Trujillo Alto: The Office Irish Pub. 7:30 pm
South Carolina
Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.
South Dakota
Sioux Falls: Empire Mall, by Burger King.
Tennessee
Knoxville: West Town Mall food court. 6 pm
Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm
Nashville: J&J's Market & Cafe, 1912 Broadway. 6 pm
Texas
Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm
Dallas: Wild Turkey, 2470 Walnut Hill Lane, outside porch near the entrance. 7:30 pm
Houston: Ninfa's Express next to Nordstrom's in the Galleria Mall. 6 pm
San Antonio: Bunsen Burger, 5456 Walzem Rd. 7 pm
Vermont
Burlington: Borders Books at Church St and Cherry St on the second floor of the cafe.
Virginia
Arlington: (see District of Columbia)
Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm
Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm.
Virginia Beach: Pembroke Mall food court. 6 pm
Washington
Seattle: Washington State Convention Center. 2nd level, south side. 6 pm
Spokane: The Service Station, 9315 N Nevada (North Spokane).
Wisconsin
Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Disrespect

United States. It's like some sort of creepy ghost story. There once were six happy payphones here. Six! All that remains now are empty shells. (And all of the people seem to have vanished, too.) Seen in Nantucket, Massachusetts.

Photo by Jules

United States. Talk about no respect. Here we have a Home Depot in Reston, Virginia that apparently thinks an empty shelf serves more of a purpose than an actual functioning payphone. We fear they may be right.

Photo by Melissa Jonas

Respect

Canada. Sure, maybe nobody's using the damn thing. But at least **it** looks attractive and artistic. So the next time you see a lonely payphone, think about making it look pretty. This one was found in Vancouver, British Columbia.

Photo by Lani Johnson

Taiwan. Someone always has to go a bit overboard, don't they? This phone, seen at TPE Airport's international terminal in Taipei, is definitely too pretty for anyone to take seriously. The Hello Kitty craze has really gotten out of hand.

Photo by Henrik

Visit **http://www.2600.com/phones/** to see our foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photos

This auto collision shop, discovered by **Kc7eph** in Seattle, is not our latest business venture. But they did manage to frame the 2600 in an almost perfect position for a future cover.

Yes, it's another 2600 building, this one found by **Jules** in Lighthouse Point, Florida. We don't know about having the solution to the national debt problem, but we do know this building is for sale and would make a dandy hacker space.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) or a *2600* t-shirt of your choice.